ANALISIS KEMANAN PROTOKOL L2TPv3 OVER IPSEC PADA SITE TO SITE VPN (VIRTUAL PRIVATE NETWORK)

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana
Jurusan Teknik Informatika

Oleh :

Nama : Aan Khusna Attabis

NIM : 06 523 234

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
YOGYAKARTA

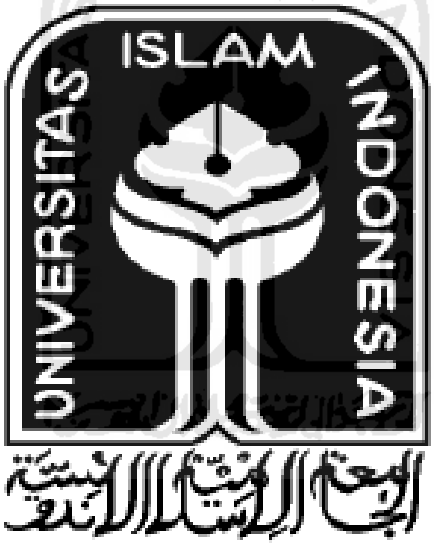
2011

HALAMAN JUDUL

ANALISIS KEMANAN PROTOKOL L2TPv3 OVER IPSEC PADA SITE TO SITE VPN (VIRTUAL PRIVATE NETWORK)

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana
Jurusan Teknik Informatika



Oleh :

Nama : Aan Khusna Attabis

NIM : 06 523 234

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
YOGYAKARTA

2011

LEMBAR PENGESAHAN PEMBIMBING

ANALISIS KEMANAN PROTOKOL
L2TPv3 OVER IPSEC PADA SITE TO SITE VPN
(VIRTUAL PRIVATE NETWORK)

TUGAS AKHIR

Oleh :

Nama : Aan Khusna Attabis

NIM : 06 523 234

Yogyakarta, 24 Maret 2011

Pembimbing

(R. Teduh Dirgahayu, ST., M.Sc.)

LEMBAR PENGESAHAN PENGUJI

ANALISIS KEMANAN PROTOKOL
L2TPv3 OVER IPSEC PADA SITE TO SITE VPN
(VIRTUAL PRIVATE NETWORK)

TUGAS AKHIR

oleh:

Nama : Aan Khusna Attabis

No Mahasiswa : 06 523 234

Telah Dipertahankan di Depan Sidang Penguji sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Jurusan Teknik Informatika
Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 24 Maret 2011

Tim Penguji

R. Teduh Dirgahayu, ST., M.Sc _____
Ketua

Syarif Hidayat, S.Kom., M.I.T. _____
Anggota I

Ari Sujarwo, S.Kom. _____
Anggota II

Mengetahui,
Ketua Jurusan Teknik Informatika
Universitas Islam Indonesia

(Yudi Prayudi, S.Si., M.Kom.)

LEMBAR PENGESAHAN PEMBIMBING

ANALISIS KEMANAN PROTOKOL
L2TPv3 OVER IPSEC PADA SITE TO SITE VPN
(VIRTUAL PRIVATE NETWORK)

TUGAS AKHIR

Oleh :

Nama : Aan Khusna Attabis

NIM : 06 523 234

Yogyakarta, 24 Maret 2011

Pembimbing

(R. Teduh Dirgahayu, ST., M.Sc.)

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR

Saya yang bertandatangan dibawah ini,

Nama : Aan Khusna Attabis

NIM : 06 523 234

Menyatakan bahwa seluruh komponen dan isi dalam Laporan Tugas Akhir ini adalah hasil karya saya sendiri. Apabila di kemudian hari terbukti ada beberapa bagian dari karya ini bukan merupakan hasil karya saya sendiri, maka saya siap menanggung resiko dan konsekuen apapun.

Demikian pernyataan ini saya buat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 24 Maret 2011

(Aan Khusna Attabis)

LEMBAR PENGESAHAN PENGUJI

ANALISIS KEMANAN PROTOKOL
L2TPv3 OVER IPSEC PADA SITE TO SITE VPN
(VIRTUAL PRIVATE NETWORK)

TUGAS AKHIR

oleh:

Nama : Aan Khusna Attabis
No Mahasiswa : 06 523 234

Telah Dipertahankan di Depan Sidang Penguji sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Jurusan Teknik Informatika
Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 24 Maret 2011

Tim Penguji

R. Teduh Dirgahayu, ST., M.Sc
Ketua

Syarif Hidayat, S.Kom., M.I.T.
Anggota I

Ari Sujarwo, S.Kom.
Anggota II

Mengetahui,
Ketua Jurusan Teknik Informatika
Universitas Islam Indonesia

(Yudi Prayudi, S.Si., M.Kom.)

HALAMAN PERSEMBAHAN

Tugas Akhir ini kupersembahkan untuk:

1. Allah SWT

Atas segala karunia dan hidayah yang telah diberikan

2. Ayah dan Ibu

Yang senantiasa memberikan segalanya yang dapat diberikan kepada anak-anaknya

3, Adek-adek ku

Yang selalu memberi warna tersediri dalam suka dan duka

MOTTO

“Dalam keadaan apapun, Allah SWT ada disekitar kita**”**

“Kebebasan bukan berarti tanpa batasan, tetapi bebas untuk menentukan batasan”

“Hidup itu cari masalah, ketemu masalah, hadapi masalah, selesaikan masalah dan hilangkan masalah tanpa masalah”

“Kesempurnaan bukan pada hasil, tetapi pada bagaimana cara kita untuk memperoleh hasil”

KATA PENGANTAR

"*Bissmillahirrohmanirrohim*"

Assalamu'alaikum Wr.Wb.

Allahamdulillahirobbil'alamin, hanya rasa sukur yang sangat mendalam yang dapat penulis panjatkan kehadirat Allah SWT, karena hanya dengan ridho dan hidayahNya penulis dapat menyelesaikan Tugas Akhir yang berjudul " Analisis Keamanan Site To Site VPN Menggunakan Protokol L2TPv3 Over IPSec" sebagai prasyarat untuk menyelesaikan masa pembelajaran jenjang Sarjana Strata 1 di jurusan Teknik Informatika Universitas Islam Indonesia.

Ada banyak sekali pembelajaran yang penulis dapatkan selama proses penyelesaian Tugas Akhir ini, dan tak lupa penulis ucapkan banyak terimakasih terhadapat pihak – pihak yang secara langsung maupun tak langsung terlibat dalam penyelesaian Tugas Akhir ini. Untuk itu penulis ingin mengucapkan ucapan terimakasih yang tulus kepada:

1. Allah SWT atas segala karunia, rahmat dan hidayahNya, juga kepada junjungan kita Nabi besar Muhammad SAW.
2. Ayahanda Tabi'in yang selalu mengajarkan nilai-nilai kehidupan di dunia maupun di akhirat kelak.
3. Ibunda Istikana yang tak pernah putus do'a, dukungan dan kasih sayang kepada putra-putrinya.
4. Adekku Tias Ismi Tamami dan Gustry Min Fadliyah yang senantiasa memberi semangat dan do'a yang tak ternilai harganya.
5. Bapak Gumbolo Hadi Susanto, Ir., M.Sc selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia.
6. Bapak Yudi Prayudi, S.Si., M.Kom. selaku Ketua Jurusan Informatika Universitas Islam Indonesia.

7. Bapak R. Teduh Dirgahayu, ST., M.Sc. selaku dosen pembimbing. Ucapan terimakasih saya haturkan atas segala bantuan, dukungan dan kesabaran yang diberikan.
8. Seluruh Dosen Jurusan Teknik Informatika Universitas Islam Indonesia yang telah mengajarkan banyak ilmu, dan semoga ilmu yang diberikan menjadi suatu nilai ibadah.
9. Teman-teman serumah, sehunian yang sudah seperti keluarga, Especially for M. Yusyuf Agus Salim (The Ustadz), Akhmad Tsabit Khoirin (Mbah Mamet), dan Novi hermawan (Mas Nopi). " *Ayo semangat buat satu kata LULUS*".
10. Sahabat-sahabat rekan seperjuangan yang special, thanks for u are Aditya Wicaksono, Barly Wicaksono, Nugroho H. Wibowo, S. Arif Wibowo, Bayu Prasetyo, Prasetyo Joko, Bobby Ermawan, Hendra Yunianto Tri Sarjana, S.Kom dan banyak lagi yang tidak dapat disebutkan satu persatu.
11. Buat Henni Ardina KD, Fibrianti Ratna Sari, " *Thanks Ya...!"*.
12. Teman-teman Teknik Informtika 2006 (FIRE), terimakasih atas pertemanan yang telah kita jalin dan semoga agan terus terjalin.
13. Semua pihak yang telah membantu dalam menyelasikan Tugas Akhir ini, "*Thanks All ot off*.."

Semoga Allah SWT senantiasa membalas semua kebaikan dan jasa-jasa yang telah diberikan dengan pahala yang berlimpah, amin.

Akhir kata penulis berharap semoga Tugas Akhir ini dapat menjadi sumber ilmu yang bermanfaat bagi siapa saja yang membacanya.

Yogyakarta, 24 Maret 2011

Penulis

ABSTRAKSI

Virtual Private Network (VPN) merupakan salah satu metode yang tepat untuk solusi keamanan jaringan dalam cangkupan *Wide Area Network* (WAN). VPN merupakan suatu cara memanfaatkan jaringan publik sebagai jaringan privat secara aman melaluai internet. Dalam penggunaan VPN, terdapat beberapa protokol *tunneling* seperti PPTP, L2F, L2TP, GRE dan IPSec. *Layer 2 Tunneling Protocol* (L2TP) merupakan salah satu protokol pilihan yang memberikan solusi keamanan pada implementasi VPN dengan cara membentuk *tunnel* (terowongan) yang menghubungkan *remote client* dengan jaringan korporat atau *site-to-site* antar jaringan korporat. Lorong yang dibuat dengan teknologi L2TP ini akan lebih aman jika di kombinasikan dengan protokol keamanan IPSec (*IP Security*) yang mampu mengenkripsi paket yang dilewatkan pada lorong atau jalur khusus tersebut.

Untuk melakukan analisis keamanan data pada implementasi *site-to-site* VPN menggunakan protokol L2TP dan IPSec, dibutuhkan simulasi untuk menunjukkan hasil implementasi dan malakukan pengujian pada pengiriman paket data. Software yang digunakan untuk melakukan simulasi ini adalah GNS3 dan VPCs. Sedangakan software yang digunakan untuk melakukan pengujian keamanan adalah wireshark yang berfungsi sebagai *sniff* .

Setelah melakukan simulasi dan pengujian keamanan komunikasi data pada *site-to-site* VPN, dapat dihasilkan nilai analisis mengenai perbandingan performance pengiriman paket data sebelum menggunakan VPN dan setelah menggunakan VPN dengan protokol tunneling L2TP dan IPSec. Juga memberikan analisis keamanan komunikasi data pada L2TP *tunneling* sebelum menggunakan IPSec dan setelah menggunakan IPSec.

Kata kunci : Virtual Private network, tunneling, Layer 2 Tunneling Protokol, IPSecurity.

TAKARIR

cryptography	salah satu metode untuk malakukan enkripsi.
gatewa	perangkat yang menjebatani dua buah jaringan.
key exchange	kunci pertukaran secara otomatis untuk autentikasi antar node.
Private	rahasia, jaringan khusus yang digunakan untuk menjaga kerahasiaan data.
Remote acces	jaringan remote akses, menghubungkan antara pengguna diluar jaringan dengan jaringan lokal.
sniff	memata-matai, kegiatan untuk memonitoring aktivitas pada sebuah jaringan.
tunnel	terowongan, metode enkapsulasi yang membungkus paket sehingga dapat dilewatkan pada jalur khusus.
virtual private network	jaringan virtual yang rahasia, membentuk jaringan lokal melaluai jaringan publik dan bersifat rahasia.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan sebuah jaringan merupakan masalah yang kompleks dalam jaringan komputer, baik jaringan lokal (*local area network* , LAN) ataupun yang terhubung dengan Internet. Untuk jaringan yang terhubung dengan Internet keamanan jaringan harus lebih mendapatkan perhatian ekstra. Pada umumnya keamanan tersebut lebih diutamakan pada server jaringan, akan tetapi komputer klien baik yang berada di dalam jaringan maupun di luar jaringan tersebut biasanya akan lebih rentan. Kerentanan ini yang dapat dimanfaatkan penyusup untuk mengakses informasi atau data dari jaringan tersebut.

Dengan adanya Internet, suatu *host* atau *client* yang berada di luar jaringan utama dapat dengan mudah terhubung dengan jaringan tersebut dengan resiko yang besar. Oleh karena itu diperlukan suatu sistem yang dapat bertukar informasi dengan aman dengan pihak yang dapat dipercaya, baik dalam jaringan local maupun jaringan Internet. *Virtual Private Network* (VPN) merupakan salah satu penyelesaian dari keamanan suatu jaringan yang mencangkup kerahasiaan, kendali akses, otentikasi, dan integritas data. VPN merupakan suatu cara menggunakan jaringan publik sebagai jaringan privat secara aman. VPN tidak didefinisikan oleh rangkaian atau rute khusus, melainkan didefinisikan oleh mekanisme keamanan dan prosedur-prosedur yang mengizinkan hanya pengguna–pengguna yang ditunjuk untuk mengakses VPN dan informasi yang mengalir melaluinya. Hal ini untuk menjaga keamanan sehingga jaringan privat tersebut tidak dapat diakses oleh pengguna yang tidak berwenang. *Layer 2 Tunneling Protocol* (L2TP) memberikan solusi keamanan dari permasalahan tersebut dengan cara membentuk *tunnel* (terowongan) pada jaringan publik yang menghubungkan *remote client* dengan jaringan korporat. Perkembangan L2TP sampai pada L2TPv3 yang memberikan solusi untuk hubungan *tunneling* dari korporat ke korporat atau dikenal dengan istilah *site-to-site* VPN.

Untuk lebih menjaga keamanan data yang melalui VPN, suatu metode seperti enkripsi data menjadi salah satu kemampuan yang harus dimiliki oleh VPN. IPsec (*Internet Protokol Security*) merupakan suatu protokol pertukaran data pada IP secara aman. IPSec dapat digunakan untuk memproteksi satu atau lebih jalur antara sepasang *host*, antara sepasang *security gateway*, atau antara *security gateway* dengan *host*.

1.2 Rumusan Masalah

Dari latar belakang di atas, rumusan masalah yang dapat dikemukakan adalah bagaimana iplementasikan teknologi *site-to-site* VPN menggunakan protokol L2TPv3 over IPSec sehingga dapat dilakukan analisis terhadap keamanan data.

1.3 Batasan Masalah

1. Implementasi VPN menggunakan L2TPv3 over IPSec dalam suatu jaringan komputer.
2. Melakukan konfigurasi L2TPV3 yang akan dikombinasikan dengan IPSec untuk jaringan *site-to-site* VPN.
3. Pengujian kinerja keamanan dari IPsec (*Internet Protocol Security*) dari sisi keamanan datanya.
4. Uji penetrasi dengan metode penyadapan data (*sniff*) dengan melakukan *capture* data menggunakan *software wireshark*.
5. Analisis bukan menitik beratkan pada perbandingan dua buah atau lebih metode tetapi mengarah pada hasil pengujian keamanan data VPN dengan IPSec sebagai protokol enkripsi datanya, yang bisa dilihat perbandingannya apabila tidak menggunakan IPSec.
6. Untuk jenis enkripsi selain yang digunakan oleh protokol IPSec tidak dibahas lebih lanjut.

1.4 Manfaat Penelitian

Adapun manfaat dari tugas akhir ini adalah:

1. Memberikan alternatif dan penjelasan implementasi jaringan VPN dalam komunikasi data secara privat.
2. Memberikan alternatif dan pengetahuan bagaimana implementasi site to site VPN dengan protokol L2TPv3 dan IPSec sebagai metode enkripsi untuk keamanan komunikasi data.

Memberikan hasil analisis terhadap tingkat keamanan protokol L2TPv3 dengan IPSec tersebut.

1.5 Tinjauan Pustaka

Tinjauan pustaka yang digunakan untuk penulisan tugas akhir ini sebagian besar berasal dari buku, riset, *white paper*, tugas akhir, dan berbagai sumber online.

Pada sebuah tugas akhir, Yulian Eka Asfihandi [ASF07] membahas mengenai *Tunneling* yang merupakan salah suatu metode mengirimkan paket data dari satu jaringan komputer ke jaringan komputer lain dengan cara membuat jalur sendiri secara privat dengan memanfaatkan jaringan Internet. Data yang dikirim akan berupa paket kecil atau *frame* yang sudah dibungkus atau dienkapsulasi sehingga tidak lagi merupakan *frame* yang sama yang dihasilkan oleh node asalnya. *Frame* ini telah dibungkus dengan *header* tambahan yang memiliki informasi routing sehingga data atau *frame* yang dikirim dapat melewati jaringan Internet. Jalur yang dilewati data dalam Internet disebut tunnel.

Pada skripsi ini akan di jelaskan implementasi VPN menggunakan protokol L2TPv3 (*Layer* 2 *Tunneling Protocol version 3*) dan protokol enkripsi IPSec, dan kemudian dilakukan analisis terhadap kemanan transfer datanya.

1.6 Metode Penelitian

Untuk memenuhi tujuan yang akan dicapai melalui penulisan skripsi ini, maka ada beberapa metode yang akan digunakan, yaitu:

1. Studi literatur dari buku – buku, makalah, ataupun manual – manual dan berbagai sumber online lainnya.
2. Implementasi VPN dengan protokol L2TPv3 dan IPSec dalam suatu jaringan.
3. Uji coba keamanan. Bertujuan untuk menganalisis tingkat keamanan transfer data pada jaringan VPN dengan protokol L2TPv3 dan IPSec tersebut.

1.7 Sistematika Penulisan

Sistematika penulisan yang digunakan pada skripsi ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang permasalahan, rumusan masalah, batasan masalah, tujuan penelitian, tinjauan pustaka, metode penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini membahas landasan teori dan mengenai konsep dasar VPN, L2TP , IPSec, autentikasi dan enkripsi.

BAB III METODOLOGI

Berisi analisis sistem dan konfigurasi yang membahas mengenai kebutuhuan perangkat keras, perangkat lunak, arsitektur sistem dan konfigurasi.

BAB IV HASIL DAN PEMBAHASAN

Berisi pengujian terhadap hasil implemenasi yang menitikberatkan pada tingkat keamanan sistem, dan pembahasan terhadap hasil yang didapatkan.

BAB V PENUTUP

Berisi tentang kesimpulan dan saran.

BAB II
LANDASAN TEORI

2.1 Virtual Private Network

2.1.1 Definisi Virtual Private Network

Jika dibahas masing-masing kata dari VPN, yaitu: *Virtual*, *Private*, dan *Network*, maka dapat diperoleh arti sebagai berikut[PAS04]:

1. *Virtual* (maya)
   a. Sumber daya jaringan yang digunakan, merupakan sumber daya yang digunakan bersama.
   b. Bukan merupakan hubungan fisik tersendiri (*physical dedicated).*
2. *Private* (privat)
   a. Kebebasan dalam pengalamatan (*addressing)* dan penentuan jalur (*routing).*
   b. Keamanan data (*authentication, encryption, integrity*).
3. *Network* (Jaringan)

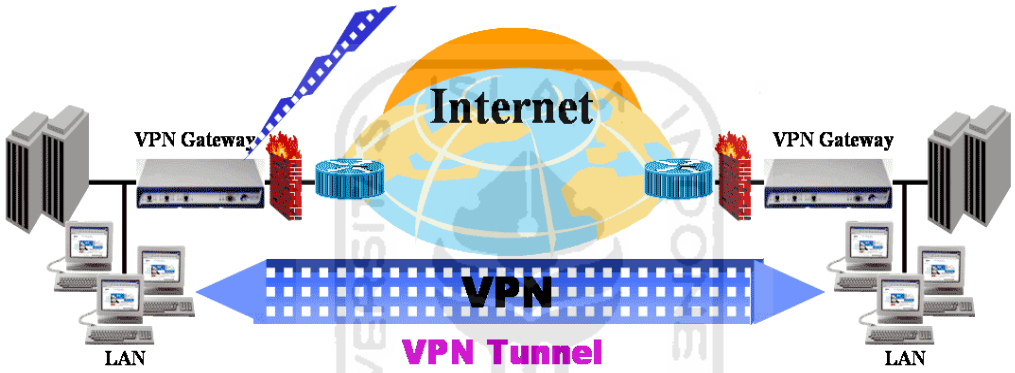
   Sekumpulan alat-alat jaringan yang saling berkomunikasi satu sama lain.

Dari penjelasan tersebut, dapat ditarik kesimpulan pengertian dari VPN adalah suatu jaringan komunikasi privat yang dibentuk pada media jaringan publik. Infrastruktur publik yang paling banyak digunakan adalah Internet, untuk memperoleh komunikasi data yang aman (*private*), diperlukan protokol khusus untuk mengatur pengamanan datanya.

Searah dengan perkembangan persaingan di dunia bisnis, menyebabkan banyak perusahaan mulai menggunakan teknologi VPN untuk membangun komunikasi dengan perusahaan lain atau perusahaan cabang ditempat yang berbeda. Perusahaan atau organisasi yang ingin membuat *wide area network* (WAN) dapat menggunakan Internet sebagai alternatifnya. Hal ini dikarenakan apabila dibandingkan dengan penggunaan *leased line* sebagai implementasi WAN tentunya akan membutuhkan investasi yang sangat besar. Diperlukan dana

pengeluran yang cukup besar apabila inigin mendapatkan hak akses istimewa menggunakan kabel untuk menghubungkan dua perusahaan tanpa bisa digunakan oleh perusahaan, organisasi atau orang lain. Akan tetapi, implementasi WAN menggunakan Internet tentunya akan membutuhkan keamanan yang lebih untuk menjaga kerahasiaan komunikasi data, VPN merupakan salah satu penyelesaian dari masalah kemamanan transfer data tersebut.

Gambaran umum dari implementasi VPN dapat dilihat pada Gambar 2.1 berikut ini.



Gambar 2.1 Koneksi VPN menggunakan jaringan Internet

Dari gambar 2.1, dapat dijelaskan bahwa koneksi VPN dibangun pada jaringan Internet. Analoginya adalah membuat jaringan yang terhubung secara Internet menjadi seolah – olah berada pada satu jaringan yang sama atau lokal. Untuk itu dibutuhkan koneksi khusus dari kedua site VPN tersebut agar dapat secara maya memiliki jalur khusus.

2.1.2 Keuntungan menggunakan VPN

Ada beberapa keuntungan yang dapat diperoleh dengan menggunakan VPN. [SAN04].

Pertama, jangkauan jaringan lokal yang dimiliki suatu perusahaan akan menjadi luas, sehingga perusahaan dapat mengembangkan bisnisnya di daerah

lain. Dengan demikian penggunaan VPN secara tidak langsung akan meningkatkan efektivitas dan efisiensi kerja.

Kedua, waktu yang dibutuhkan untuk menghubungkan jaringan lokal ke tempat lain tidak lama, karena proses instalasi infrastruktur jaringan dilakukan perusahaan atau kantor cabang yang baru dengan ISP (*Internet service provider*) terdekat di daerahnya. Sedangkan pada penggunaan *leased line* sebagai WAN membutuhkan waktu yang lama untuk membangun jalur koneksi khusus dari kantor cabang yang baru ke kantor pusat.

Ketiga, penggunaaan VPN di dunia Internet, dapat mereduksi biaya operasional bila dibandingkan dengan penggunaan *leased line* untuk mengimplementasikan WAN. VPN tidak membutuhkan kabel tersendiri yang panjang, sehingga tidak membutuhkan biaya yang sangat besar. Karena VPN menggunakan Internet sebagai media komunikasi perusahaan hanya membutuhkan kabel yang relatif pendek untuk menghubungkan perusahaan tersebut dengan ISP terdekat.

Keempat, karena VPN merupakan solusi keamanan pada implementasi WAN menggunakan Internet, tentunya akan memberi kemudahan akses bagi pengguna VPN tersebut. Sebagai contoh pegawai yang selalu berpindah dari satu tempat ke tampat lain, dapat mengakses jaringan khusus perusahaan di manapun dia berada, selama dia bisa mendapatkan akses Internet. Hal ini tidak dapat dilakukan jika perusahaan menggunakan *leased line* yang hanya dapat diakses pada terminal tertentu saja.

2.1.3 Kerugian Menggunakan VPN

Selain kelebihan-kelebihan tersebut, VPN juga memiliki kelemahan sebagai berikut[SAN04].

Pertama, VPN membutuhkan perhatian yang serius. Oleh karena itu diperlukan tindakan yang tepat untuk mencegah terjadinya hal-hal yang tidak diinginkan seperti penyadapan, *hacking* dan tindakan *cyber crime* pada jaringan VPN.

Kedua, ketersediaan dan kinerja VPN sangat tergantung pada faktor-faktor yang berada di luar kendali pihak perusahaan. Kecepatan dan keandalan transmisi data melalui Internet yang digunakan sebagai media komunikasi jaringan VPN tidak dapat diatur sepenuhnya oleh pihak pengguna jaringan VPN, karena lalulintas yang terjadi di Internet melibatkan pengguna Internet lain.

Ketiga, perangkat pembangun teknologi jaringan VPN dari beberapa vendor yang berbeda memungkinkan perangkat–perangkat tersebut tidak dapat saling berinteroperasi karena standard teknologi VPN belum memadai. Oleh karena itu, fleksibilitas dalam memilih perangkat yang sesuai dengan kebutuhan dan keuangan perusahaan sangat kurang.

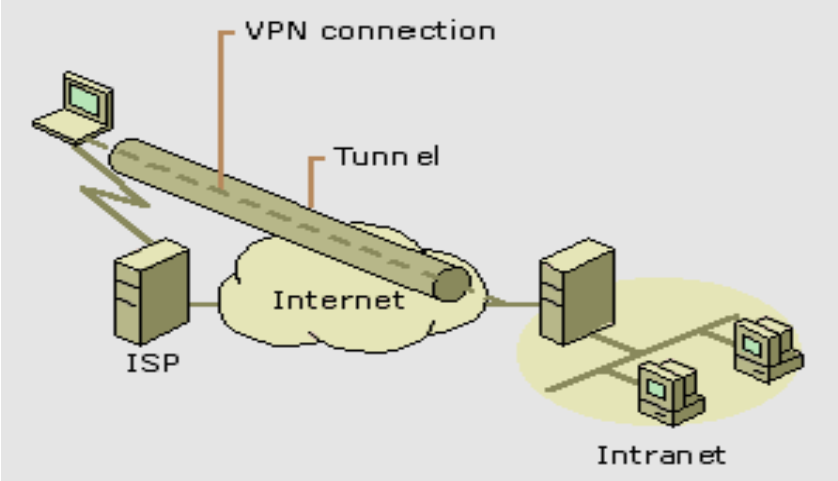
2.1.4 Jenis Inplementasi VPN

Pada umumnya implementasi VPN terdiri dari 2 macam. Pertama adalah *remote access* VPN, dan yang kedua adalah s*ite-to-site* VPN.

2.1.4.1 Remote Access VPN

Remote access VPN biasa juga disebut *virtual private dial-up network* (VPDN), VPN ini menghubungkan antara pengguna di luar jaringan dengan suatu jaringan lokal. VPN ini digunakan oleh pegawai perusahaan yang ingin terhubung ke jaringan lokal perusahaannya dari lokasi yang jauh (*remote*) dari perusahaannya. Biasanya perusahaan yang ingin membuat jaringan VPN 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 [SAN04].

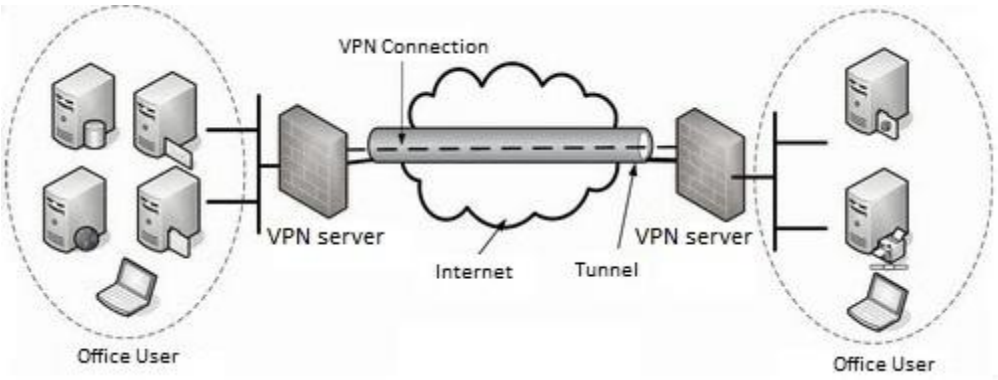
Perusahaan yang memiliki pegawai yang ada di lapangan dalam jumlah besar dapat menggunakan *remote access* VPN untuk membangun koneksi WAN melalui Internet. VPN tipe ini akan memberikan keamanan antara jaringan lokal perusahaan dengan pegawai yang ada di lapangan. Pihak ketiga yang membantu hubungan ini adalah ISP. Untuk contoh topologinya dapat diliat dalam gambar 2.2 berikut.



Gambar 2.2 VPN dengan Remote Access VPN

2.1.4.2 Site-to-site VPN

VPN ini menghubungkan antara dua atau lebih kantor 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**. VPN yang digunakan untuk menghubungkan kantor pusat dengan kantor cabangdisebut **intranet** *site-to-site* VPN [SAN04]. Contoh topologi *site-to-site* VPN dapat dilihat pada gambar barikut.



Gambar 2.3 VPN dengan Sie-to-site VPN

2.1.5 VPN Tunneling

Menurut Mairs, 2002, *tunneling* merupakan metode untuk transfer data dari satu jaringan ke jaringan yang lain dengan memanfaatkan jaringan Internet secara terselubung [AFS07].

Untuk menjamin komunikasi yang aman antara dua buah segmen jaringan, yaitu jaringan lokal perusahaan dan jaringan luar perusahaan atau klien yang berpindah melalui jaringan publik (Internet), maka teknologi *tunneling* dan enkripsi dilakukan pada penerapan VPN.

Dengan *tunneling*, antara kedua segmen jaringan VPN dapat berkomunikasi satu sama lain dengan membuat suatu lorong (*tunnel*) khusus menggunakan protokol *tunneling* yang sama. Penerapan enkripsi pada VPN membuat data-data perusahaan tidak terbaca oleh *sniffer*[PAS04].

Teknologi VPN dikelompokan secara garis besar berdasarkan protokol *tunneling* lapisan 2 (Data Link Layer) dan lapisan 3 (Network Layer) pada model OSI. Lapisan 2 (*layer 2*) terdiri dari L2F (*Layer 2 Forwarding*), PPTP (*Point to Point Tunneling Protocol*) dan L2TP (*Layer 2 Tunneling Protocol*). Lapisan 3 (*layer 3*) antara lain IPSec (*IP Security*) dan GRE (*Generate Routing Encapsulation*).

L2TP adalah salah satu standar IETF (*Internet Engineering Task Force*) (RFC 2661) pada lapisan 2 yang merupakan kombinasi dari L2F dan PPTP yang didukung oleh vendor–vendor, misalnya: Ascend, Cisco, IBM, Microsoft dan 3Com. Untuk mendapatkan tingkat keamanan yang lebih baik, L2TP dapat dikombinasikan dengan *tunneling* IPSec pada lapisan 3.

2.2 Layer 2 Tunneling Protocol (L2TP)

2.2.1 Definisi L2TP

L2TP adalah protokol layer 2 yang mengkombinasikan keunggulan-keunggulan fitur protokol L2F (*Layer 2 Forwarding*) yang di kembangkan oleh Cisco dan PPTP (*Point-to-Point Tunneling Protocol*) yang dikembangkan oleh Microsoft, L2TP menyediakan akses *remote dial-up* ke suatu jaringan korperasi dengan beragam *protocol* dan terenkripsi melalui Internet [ASF07].

Protokol L2TP sering juga disebut sebagai protokol *dial-up* virtual, karena L2TP memperluas suatu sesi dial-up PPP (Point-to-point Protocol) melalui jaringan publik Internet. L2TP sering juga disebut sebagai koneksi virtual PPP. L2TP bisa mempunyai beberapa saluran dengan *Quality of Service* (QOS) yang berbeda-beda. L2TP mampu bekerja pada jaringan non-IP. Walau demikian, ketika proses transfer data berjalan di atas IP jaringan, *freme – frame* L2TP dienkapsulasi di dalam UDP. Dengan menggunakan *port* UDP 1701, *tunnel* L2TP memanfaatkan satu *port* UDP *source*/asal (yang bukan 1701) dan mengirimkan ke tujuan yang di kehendaki dengan alamat *port* 1701.

2.2.2 Perangkat L2TP

Perangkat dasar L2TP antara lain:

1. Remote Client
   - Suatu sistem atau *router* pada jaringan klient.
2. L2TP Access Concentrator (LAC)
   - Sistem yang berada disalah satu ujung *tunnel* L2TP dan merupakan peer ke LNS.
   - Berada disisi *remote client* / ISP.
3. L2TP Network Server (LNS)
   - Sistem yang berada disalah satu ujung *tunnel* L2TP dan merupakan peer ke LAC.
   - Berada pada sisi jaringan korporat.

2.2.3 Tunnel L2TP

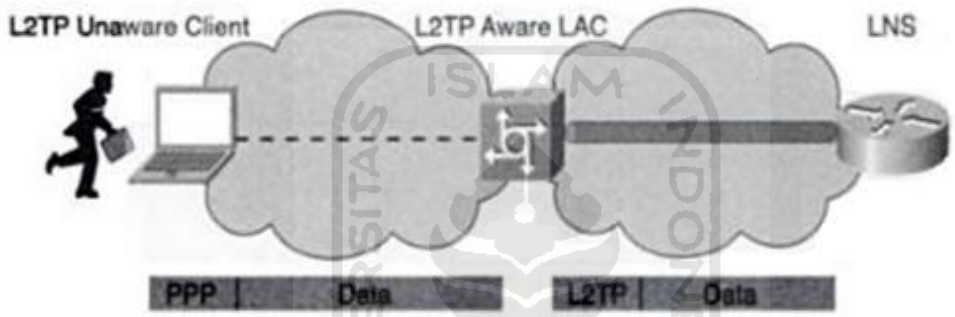
Skenario L2TP adalah untuk membentuk *tunnel* atau terowongan frame antara *remote client* dengan LNS yang berada pada suatu jaringan korporat.

Pada perkembangannya, sistem *tunneling* L2TP mengalami banyak sekali perubahan dan penambahan protokol. Pada mulanya L2F didefinisikan sebagai L2TP versi 1, kemudian terus berkembang menjadi L2TPv2 dan hingga saat ini berkembanglah L2TPv3.

Terdapat dua model *tunnel* yang dikenal, yaitu *compulsory* dan *voluntary*. Perbedaan utama diantara keduanya terletak pada *end point tunnel*-nya. Pada *compulsory tunnel* ujung *tunnel* berada pada ISP,sedangkan pada *voluntary* ujung *tunnel* berada pada *client remote*[PAS04].

2.2.3.1 Model Compulsory L2TP

Model : (Client) → PPP + Data →(LAC) → L2TP + Data → (LNS), atau dijelaskan pada gambar 2.4 berikut.

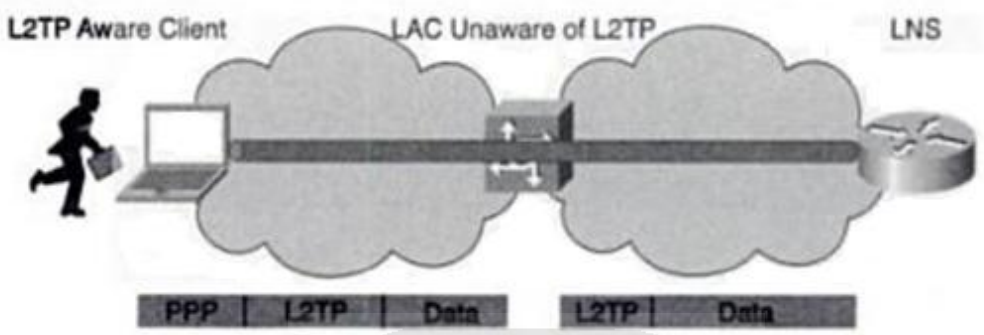


Gambar 2.4 Model Compulsary L2TP

1. *Remote client* memulai meminta koneksi PPP (*Point-to-Point Protocol*) ke LAC.
2. LAC menerima koneksi tersebut.
3. LAC melakukan autentikasi.
4. LAC kemudian meresmikan *tunnel* L2TP ke LNS.
5. Jika LNS menerima koneksi, LAC kemudian membungkus PPP dengan L2TP, dan meneruskannya melalui tunnel yang tepat.
6. LNS menerima frame-frame tersebut, kemudian membuka paket yang dibungkus protokol L2TP, dan memprosesnya sebagai frame PPP biasa.
7. LNS kemudian menggunakan pengesahan PPP untuk melakukan validasi user.

2.2.3.2 Model Voluntary L2TP

Model : (Client) → PPP + L2TP + Data → (LAC) → L2TP + Data → (LNS), atau dijelsakan pada gambar 2.5 berikut.



Gambar 2.5 Model Voluntary L2TP

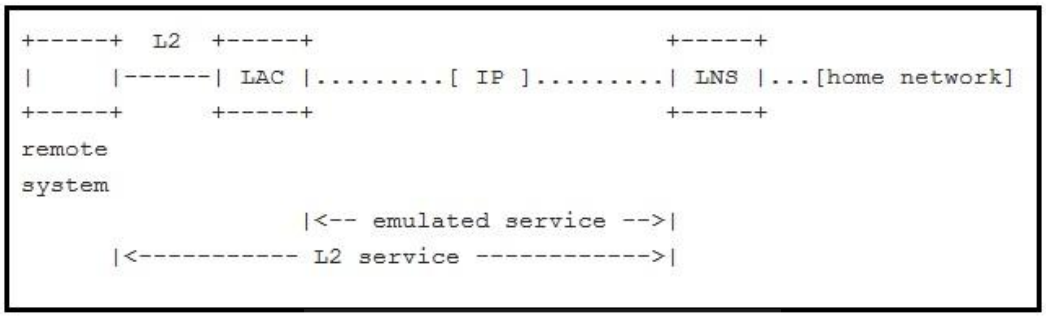
1. *Remote Client* befungsi juga sebagai LAC.
2. *L2TP Acces Client* (LAC) meresmikan *tunnel* L2TP ke LNS.
3. Jika LNS menerima koneksi, LAC kemudian membungkus paket PPP dengan L2TP, dan meneruskannya melalui *tunnel*.
4. LNS menerima frame-frame tersebut, kemudian membuka paket yang dibungkus L2TP, dan memprosesnya sebagai frame PPP biasa.

2.2.4 L2TPv3

Dalam perkembangan teknologi L2TP, banyak fitur-fitur tambahan yang mendorong munculnya L2TPv3. L2TPv3 adalah perkembangan dari teknologi L2TP yang memiliki beberapa manfaat seperti menyederhanakan penyebaran VPN misal dengan hanya menghubungkan antar korporat, L2TPv3 juga tidak membutuhkan MPLS sehingga dapat mengurangi pengeluaran biaya, L2TPv3 mendukung *tunneling* lapisan 2 *over* IP untuk muatan apapun. Ada 3 mode L2TPv3 yaitu:

1. LAC – LNS

Sama dengan kemampuan teknologi L2TP pada dasarnya untuk melakukan hubungan *remote access* dari LAC ke LNS. Dapat dilihat pada gambar 2.6 berikut.



Gambar 2.6 L2TPv3 Model LAC-LNS [RFC3931]

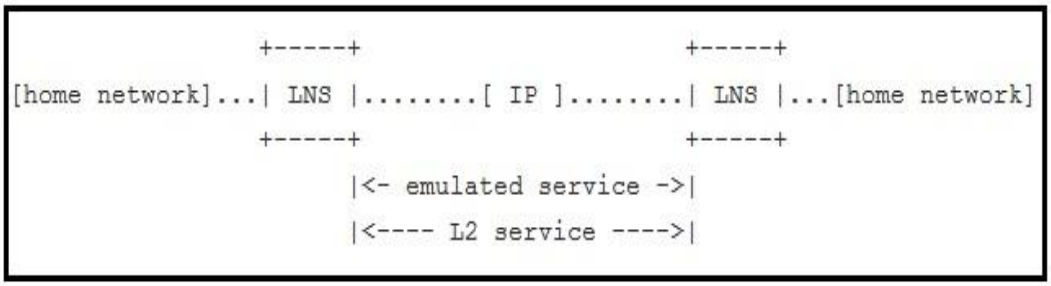
2. LAC – LAC

Melakukan hubungan simetris dimana antara kedua LAC dapat saling malakukan *remote access*. Dapat dilihat pada gambar 2.7 berikut.

Gambar 2.7 L2TPv3 Model LAC-LAC [RFC3931]

3. LNS – LNS

Menghubungkan site-to-site VPN misal antara korporat dengan korporat. Komputer pada home *network* yang ada di belakang LNS tidak harus melakukan *tunneling* lapisan 2, Model LNS-LNS dapat dilihat pada gambar 2.8 berikut.



Gambar 2.8 L2TPv3 Model LAC-LNS [RFC3931]

2.3 IP Security (IPSec)

2.3.1 Definisi IPSec

IPSec menyediakan layanan keamanan pada lapisan IP dengan mengizinkan sistem untuk memilih protokol keamanan yang diperlukan, menentukan algoritma yang akan digunakan pada layanan, dan menempatkan kunci kriptografi yang diperlukan . IPSec dapat digunakan untuk melindungi satu atau lebih jalur antara sepasang *host*, antara sepasang *security gateway*, atau antara *security gateway* dengan *host*.

2.3.2 Cara Kerja IPSec

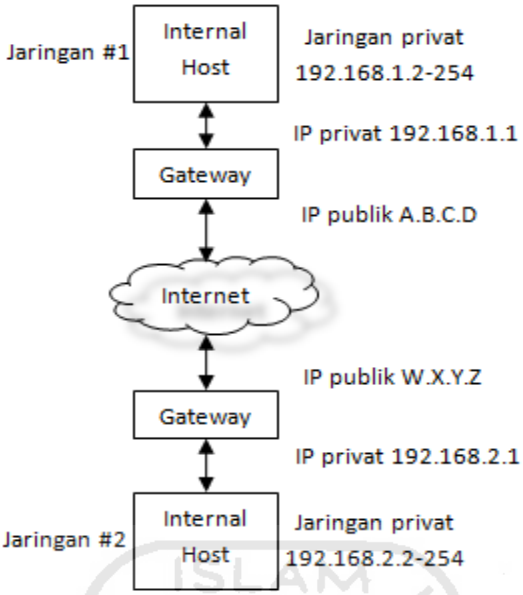
Untuk membuat sebuah sesi IPSec, dibutuhkan sebuah framework protokol ISAKMP/Oakley. Framework tersebut mencakup beberapa algoritma kriptografi, dan dapat diperluas dengan menambahkan sistem kriptografi tambahan yang dibuat oleh pihak ketiga. Selama proses negosiasi dilakukan, persetujuan akan tercapai dengan metode autentikasi dan kemanan yang akan digunakan, dan protokol pun akan membuat sebuah kunci yang dapat digunakan bersama (shared key) yang nantinya digunakan sebagi kunci enkripsi data. IPSec menggunakan dua protokol untuk menyediakan layanan keamanan lalulintas yaitu Authentication Header (AH) and Encapsulating Security Payload (ESP).

a. **Protokol Authentication Header (AH):** protokol ini menawarkan autentikasi pengguna dan perlindungan dari beberapa macam serangan (umumnya serangan man in the middle). Protokol AH juga menyediakan fungsi autentikasi dan integritas data. Dengan protokol ini penerima dapat

merasa yakin bahwa identitas si pengirim adalah benar, dan data tidak dimodifikasi selama transmisi. Namun demikian, protokol AH tidak mempunyai fungsi enkripsi terhadap data yang ditransmisikannya. Informasi AH dimasukkan ke dalam header paket IP. Protokol AH dapat digunakan secara tersendiri atau bersamaan dengan protokol Encapsulating Security Payload.

b. **Protokol Encapsulating Security Payload (ESP):** protokol ini melakukan enkapsulasi dan enkripsi data untuk meningkatkan kerahasiaan data. Protokol ESP juga dapat memiliki skema autentikasi dan perlindungan dari beberapa macam serangan. ESP dapat digunakan secara tersendiri atau bersamaan dengan protokol Authentication Header. informasi ESP dimasukkan ke dalam header paket IP .
c. Kedua protokol ini merupakan pembawa kontrol akses berbasis distribusi kunci kriptografi dan manajemen aliran lalulintas relatif terhadap protokol keamanan.

Protokol-protokol ini dapat diterapkan pada IPv4 dan IPv6. Masing-masing protokol mendukung dua mode penggunaan mode transport dan mode tunnel. Dalam mode transport, protokol menyediakan proteksi terutama untuk protokol lapisan berikutnya. Sedangkan dalam mode tunnel, protokol diterapkan untuk meneruskan paket IP. Mode transport mengkripsi bagian data (*payload*) masing-masing paket tanpa mengubah *header* paket tersebut. Algoritma yang digunakan adalah algoritma kriptografi simetris. IPSec mode ini menggunakan sub-protokol yang disebut sebagai *encapsulated security payload (*ESP).Pada mode *tunnel,* data dan *header* paket yang dikirim dihitung menggunakan teknik *checksum* kriptografi. Bagian *header* paket IP tersebut kemudian ditambahi *checksum* agar bisa diautentikasi di bagian penerima. Mode ini seolah-olah membuat lorong khusus pada jaringan publik yang hanya dapat diakses oleh orang-orang tertentu. Contoh diagram penggunaan IPSec untuk menghasilkan komunikasi yang aman menggunakan jaringan publik ditunjukkan pada gambar 2.9.



Gambar 2.9 Contoh Implementasi IPSec

Pada gambar 2.9 di atas, jaringan privat #1 menggunakan IP privat, begitu juga dengan jaringan privat #2. Sedangkan kedua *gateway* menggunakan IP publik yang bisa diakses dari mana saja. Untuk dapat melakukan perintah ping dari jaringan internal #1 ke jaringan internal #2, ada beberapa tahapan yang harus dilalui.

1. Setiap paket yang dikirim ke IP 192.168.2.1 dibungkus dalam paket lain sehingga *header* IP yang muncul adalah IP A.B.C.D. Kemudian paket ini dikirim ke IP W.X.Y.Z melalui *gateway* dengan *header* IP yang menyatakan seolah-olah paket berasal dari IP A.B.C.D. Proses ini disebut sebagai proses enkapsulasi paket.
2. *Gateway* harus mengetahui jalan untuk mencapai IP 192.168.2.1. dengan kata lain, *gateway* harus mengarahkan paket ke IP 192.168.2.1
3. Paket yang tiba di IP W.X.Y.Z harus di enkapsulasi sehingga diperoleh paket yang sebenarnya dan dikirim ke alamat IP 192.168.2.1.

Proses ini membuat jalur khusus atau lorong antara dua jaringan. Dua ujung jalur ini berada di alamat IP A.B.C.D dan W.X.Y.Z. Lorong ini harus diberi aturan yang mengizinkan alamat IP mana saja yang boleh melalui lorong ini.

Apabila koneksi telah terbentuk, perintah ping 192.168.2.1 yang dilakukan ke komputer dengan IP 192.168.1.1 akan mendapat balasan (*reply*).

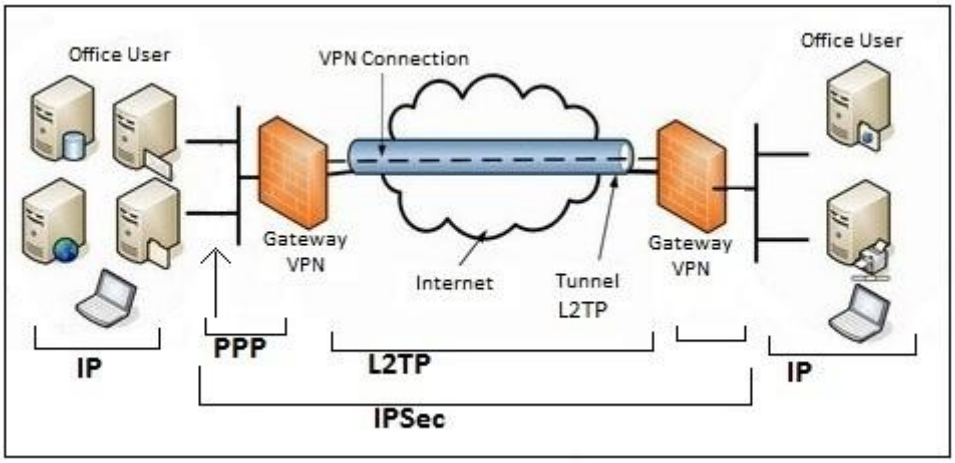
BAB III
METODOLOGI

3.1 Analisis Sistem.

3.1.1 Deskripsi Sistem

Dari latar belakang yang diuraikan sebelumnya, perancangan VPN pada penelitian ini akan memanfaatkan teknologi IPSec sebagai protokol keamanan datanya. Sedangkan teknologi *Tunneling* yang merupakan terowongan dari korporat 1 menuju korporat 2 menggunakan *Protocol* L2TPv3. Sistem yang dibangun bertujuan menghubungkan antara dua buah router secara *site-to-site VPN*.

Site–to-site VPN dapati menggambarkan komunikasi data antara sebuah perusahaan dengan perusahaan cabang yang ada di luar kota. Komunikasi data tersebut akan melibatkan protokol L2TP sebagai jalur *tunneling* sehingga komputer user dari perusahaan 1 dapat berkomunikasi dan bertukar data dengan komputer user pada perusahaan 2 sebagai mana suatu intranet atau *lokal area network*. Paket yang melewati hubungan *tunneling* tersebut dibungkus secara aman dengan protokol IPSec. Protokol ini melindungi komunikasi data dari user ke *gateway* dan dari *gateway router* ke *gateway router* berikutnya sehingga kerahasiaan paket data dari masing – masing perusahaan tersebut dapat dipastikan aman. Perjalanan protokol L2TP dan Protokol IPSec secara umum dapat ditunjukkan pada gambar 3.1.



Gambar 3.1 Site-to-site VPN dengan L2TP over IPSec

Komponen – komponen yang digunakan dalam sistem ini adalah sebagai berikut:

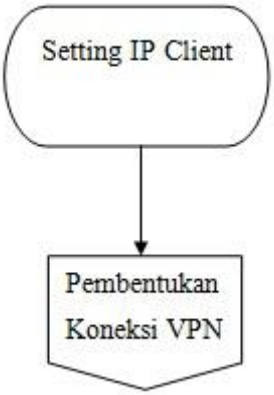
1. L2TP, merupakan protokol enkapsulasi paket data dengan teknologi (*tunneling*) yang membungkus paket agar dapat diterima oleh end point. Tujuan enkapsulasi adalah menginisiasi dan menyesuaikan kondisi paket agar bisa dilewatkan pada *tunnel* yang disediakan.
2. IPsec, digunakan sebagai penyedia layanan pengamanan kriptographi *(cryptographie security service)* dan mengautentikasi paket pada lapisan IP. IPSec membungkus paket yang melewati *tunneling* L2TP sehingga identitas paket dan jalur yang digunakan dapat dirahasiakan.
3. PPP, digunakan dalam mekanisme enkapsulasi untuk membungkus paket - paket *multiprotocol* melalui hubungan *point-to-point* pada lapisan 2.

3.1.2 Proses Perjalanan Sistem

Proses atau urutan langkah – langkah akan digambarakan melalui diagram alir atau yang disebut dengan *Flow Chart*.

3.1.2.1 Proses Pada Sistem Client

Berikut digambarkan proses sistem *client* secara gambaran umum, yang terdiri dari sebuah sub - proses.



Gambar 3. 2 Proses pada Client

Pada laporan ini proses client dilakukan oleh *Virtual PC Simulator* (VPCS) yang hanya menampilkan layar CMD (*Comand Prompt Windows*). Setelah koneksi VPN terbentuk, maka antara komputer klien pada jaringan satu dan komputer klien pada jaringan dua akan terhubung seperti pada LAN (Local Area Network) meskipun berada pada jaringan yang terpisah.

3.1.2.2 Proses Pada Server

Proses pada server berjalan pada dua buah router Cisco sebagai VPN *gateway* yang terhubung secara *site-to-site* VPN dengan model LNS-LNS, dapat dijelaskan pada diagram alir berikut.

Gambar 3. 3 Proses pada Server

Adapun sub-proses pada gambar 3.3 dapat dijelaskan sebagai berikut:

a. Negoisasi Tunnel L2TP

   Negoisasi ini berperan penting dalam tahapan membentuk L2TP tunnel yang menghubungkan VPN.

b. Negoisasi sesi L2TP

   Proses ini digunakan oleh LNS1 untuk mem-*forward* data autentikasi user menuju LNS2 atau sebaliknya dengan menggunakan L2TP tunnel yang telah terbentuk diantara LNS1 dan LNS2. Setelah negoisasi terbentuk, maka antara komputer klien pada jaringan 1 dan komputer klien pada jaringan 2 dapat membentuk hubungan *peer-to-peer* sehingga dapat melakukan pertukaran data melalui tunnel L2TP.

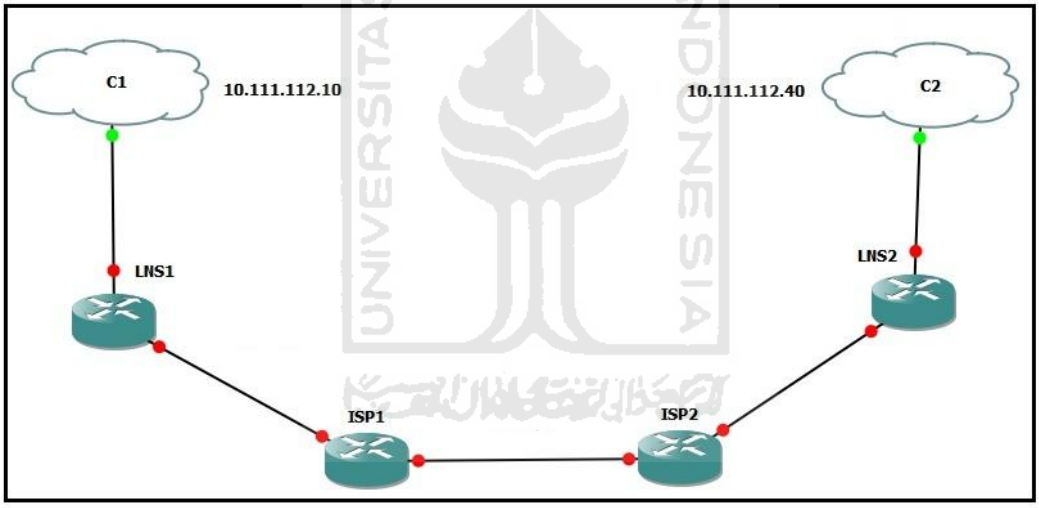
c. Negoisasi IPSec

Setelah terbentuknya tunnel L2TP dan sesi L2TP, menandakan bahwa komputer klien pada jaringan 1 telah terhubung dengan komputer klien pada jaringan 2 melewati jaringan intranet yang akan melalui dua buah ISP. Apabila prosedur ini sudah terbentuk secara sempurna, maka user dapat mengakses *gateway server* VPN dengan kondisi aman dari gangguan pihak – pihak yang tidak diharapkan.

3.2 Implementasi Sistem

3.2.1 Ruang Lingkup Sistem

Gambaran umum sistem dijelaskan pada gambar 3.4 sebagai berikut.



Gambar 3. 4 Gambaran Umum Sistem

Sistem VPN yang diimplementasikan terdiri dari dua buah *router gateway* yang melewati dua buah ISP. Masing-masing *router gateway* tersebut terhubung ke user sebagai klien user. Koneksi antara dua buah *router gateway* tersebut memanfaatkan teknologi *tunneling* dengan L2TPv3 dan enkripsi paket data dengan IPSec. Dua buah *router gateway* tersebut di implementasikan dengan Cisco router pada software simulasi jaringan GNS3. Sedangkan implementasi klien menggunakan *tools* virtual PC yaitu VPCS.

3.2.2 Perangkat Lunak Sistem

Perangkat lunak yang dibutuhkan adalah sebagai berikut.

a. GNS3
b. VPCS
c. WinPcap
d. Wireshark

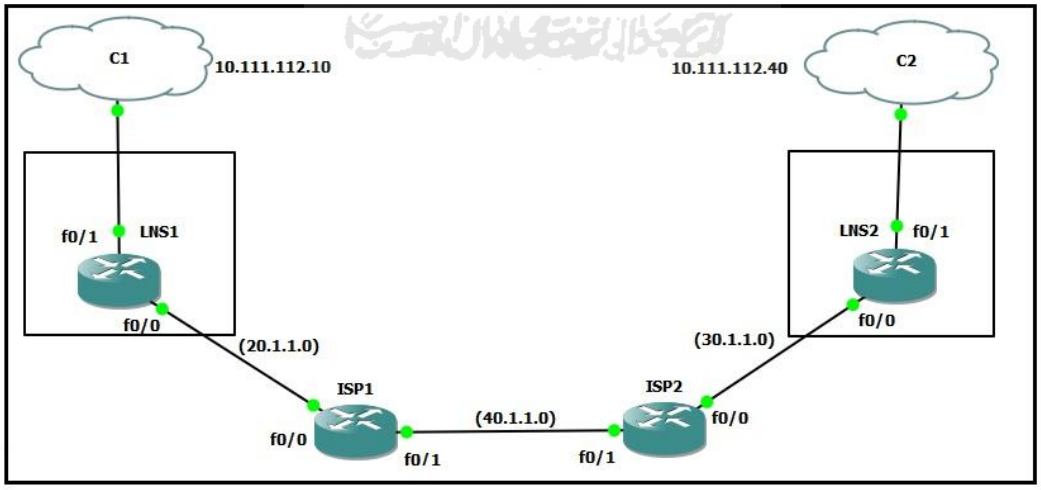
3.2.3 Perangkat Keras Sistem

Komponen perangkat keras yang akan disimulasikan adalah sebagai berikut:

a. 2 buah router gateway (LNS)
b. 2 buah router ISP
c. 2 buah PC client

3.2.4 Arsitektur Jaringan

Penelitian ini akan menggunakan emulator CISCO IOS 3700 sebagai salah satu produk dari CISCO yang mempunyai fasilitas VPN. Sistem yang diimplementasikan pada simulator GNS3 dapat dijelaskan pada gambar 3.4.



Gambar 3. 5 Arsitektur Jaringan VPN L2TPv3 Over IPsec

Berdasarkan Gambar 3.5, setelah *client* yang berada pada masing - masing *client 1* dan *client 2* melakukan koneksi ke LNS1 atau LNS2, L2TPv3 akan menjabarkan autentikasi user yang telah diberi alokasi alamat IP, LNS1 akan memvalidasi user yang terhubung dan melakukan *xconnect* kepada *interface fast ethernet 0/1* pada LNS2 dan begitu sebaliknya. Sehingga metode *site-to-site* denagn model LNS-LNS akan terbentuk pada kedua *router gateway* tersebut. Setelah koneksi *tunnel* L2TPv3 terbentuk antara LNS1 ke LNS2 maka *client 1* dan *client 2* dapat berkomunikasi seakan - akan berada pada satu jaringan lokal. Paket data yang akan dipertukarkan melalui *tunnel* tersebut dilindungi secara aman oleh teknologi IPSec.

Berdasarkan pada arsitektur jaringan yang dibuat, maka dirancang parameter jaringan sebagai berikut:

a. Gateway VPN (LNS)

- LNS1

  ip publik : 20.1.1.2 netmask 255.255.255.0

  gateway : 20.1.1.1

  ip private : unassigned

- LNS 2

  ip publik : 30.1.1.2 netmask 255.255.255.0

  gateway : 30.1.1.1

  ip private : unassigned

b. Client VPN

- Client 1

  Ip network : 10.111.112.10

  Gateway : 10.111.112.1

- Client 2

  Ip network : 10.111.112.40

  Gateway : 10.111.112.1

c. ISP

- ISP 1

  ip network : 20.1.1.1 netmask 255.255.255.0

- ISP 2

  ip network : 30.1.1.1 netmask 255.255.255.0

3.2.5 Konfigurasi Sistem

Sistem konfigurasi yang tepat diperlukan agar komputer *client* dapat digunakan sebagaimana dengan kebutuhan pengguna. Hal ini ditandai dengan terbentuknya koneksi data yang aman dari *user client 1* ke *user client 2* secara intranet.

3.2.5.1 Konfigurasi LNS 1

Konfigurasi L2TPv3 diawali dengan menentukan nama *l2tp-class,* disini misal nama *l2tp-class* yang digunakan adalah *test. L2tp-clas* merupakan konfigurasi untuk mendefinisikan parameter autentikasi dan kontrol terhadap L2TP. Parameter yang diatur pada *l2tp-class* antara lain *hello, retrasmit,* dan *cookie*.

Hello packet digunakan untuk mengetahui keadaan router tetangganya apakah masih hidup aau sudah mati. *Hello* 10 berarti mengirimkan *packet hello* dalam skala 10 detik sekali. Parameter *retransmt* menetapkan berapa kali router akan mencoba untuk mengirimkan kontrol paket awal untuk pembentukan terowongan sebelum menyatakan *router* dalam keadaan sibuk, disini digunakan "*retransmit initial retries 30*" atinya, router akan mencoba mengirimkan kontrol paket L2TPv3 awal sebanyak 30 kali. *Cookie size* digunakan untuk mendefinisikan lebar terowongan, disini hanya ada dua pilihan yaitu 8 atau 4.

```
l2tp-class test
 hello 10
 retransmit initial retries 30
 cookie size 8
```

Setelah itu dilanjutkan dengan configurasi *pseudowire-class* dengan memberi nama *pseudowire-class* nya, misal disini diberi nama "*test"*. *Pseudowire-class* merupakan parameter untuk mendefinisikan mode enkapsulasi, protokol *tunneling,* dan *interface* yang akan akan digunakan oleh *tunnel* L2TPv3 over

IPSec. *Interface* yang akan digunakan adalah *interface loopback1*. Konfigurasi parameter *pseudowire-class* adalah sebagai berikut.

```
pseudowire-class test
 encapsulation l2tpv3
 protocol l2tpv3 test
 ip local interface Loopback1
```

Konfiguasi selanjutnya menentukan menentukan parameter IPSec yang akan digunakan. Hal ini dengan membuat IKE policy kemudian menentukan parameter-parameter seperti metode enkripsi, autentikasi dan group yang akan digunakan. IKE *name* yang digunakan adalah "cisco".

```
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
 crypto isakmp key cisco address 0.0.0.0 0.0.0.0
```

Selanjutnya adalah konfigurasi *transform set* untuk mengarahkan *tunneling* IPsec. Konfigurasi yang dilakukan adalah memberi nama *transform set* misal "VPN" dan memberikan parameter *cyrpto map* untuk menentukan arah *tunneling* IPSec. Parameter – parameter tersebut antara lain : set peer destination, yaitu IP publik pada LNS 2 yang dalam ujicoba ini digunakan alamat IP 30.1.1.2. Kemudian menentukan menentukan *set transform* dan *match address transform*.

Transform set digunakan untuk mendefinisikan jenis kriptography yang akan digunakan, menggunakan *esp-sha-hmac*.

```
crypto ipsec transform-set vpn esp-3des esp-sha-hmac
!
crypto map vpn 10 ipsec-isakmp
 set peer 30.1.1.2
 set transform-set vpn
 match address vpn
```

Konfigurasi selanjutnya adalah memberikan alokasi alamat IP pada *interface – interface* yang digunakan, yakni *interface loopback1*, *interface fastethernet0/0*, dan *interface fastethernet0/1*.

```
interface Loopback1
 ip address 10.1.1.1 255.255.255.0
 no shutdown
!
interface FastEthernet0/0
 ip address 20.1.1.2 255.255.255.0
 duplex auto
 speed auto
 no shutdown
 crypto map vpn
```

Pada *interface fastethernet0/1* ditambahkan parameter *xconnect* yang mampu mennggantikan kebutuhan dasar seperti *keep alive* dan *peer destination*. Pada definisi ini *xconnect* berperan untuk memperkenalkan protokol L2TPv3 dan *pw-class* melalui sesi pengenalan IPSec menuju interface *loopback1* pada LNS2 dengan alamat IP 10.1.4.1. hal ini dilakuakan duapaya *host* dibelakang LNS dapat saling berkomunikasi sesuai dengan model L2TPv3 yaitu LNS-LNS.

Konfigurasi “xconnect 10.1.4.1 100 encapsulation l2tpv3 pw-class test” artinya *interface* ini menampung parameter manual yang menetapkan bahwa akan digunakan L2TPv3 sebagai metode pseudowire tunnelingnya, dan melewati metode komunikasi *xconnect*.

```
interface FastEthernet0/1
 description LAN
 no ip address
 no shutdown
 duplex auto
 speed auto
 no cdp enable
 xconnect 10.1.4.1 100 encapsulation l2tpv3 pw-class test
```

Kemudian mengatur parameter *acces list* untuk menerangkan *traffic* jaringan yang bisa diterima atau diteruskan oleh *interface* dari router. Dengan membuat acces list ini secara tidak langsung mengandung statemen "deny all" yang menolak alamat IP lain selain yang ada pada statemen permit.

```
ip access-list extended vpn
  permit ip host 10.1.1.1 host 10.1.4.1
```

Konfigurasi terakhir adalah menentukan *routing* untuk jalur menuju ISP 2 melewati IPS 1.

```
ip route 0.0.0.0 0.0.0.0 20.1.1.1
```

Skrip lengkap konfigurasi pada *router 1* terlampir.

3.2.5.2 Konfigurasi LNS 2

Konfigurasi LNS2 tidak jauh berbeda dengan konfigurasi LNS1. Konfigurasi menggunakan tahapan – tahapan yang sama yaitu menentukan parameter *l2tp-class, pseudowire-class,* parameter IPSec, dan alokasi *interface* yang digunakan. Nama *l2tp-class* yang digunakan sama yaitu "test", kemudian menetapkan berapa jumlah paket *hello* dan berapa kali router akan mencoba mengirimkan kontrol paket awal untuk pembentukan terowongan sebelum menyatakan *router* dalam keadaan sibuk dengan perintah *retransmit*. Konfigurasinya adalah sebagai berikut.

```
l2tp-class test
 hello 10
 retransmit initial retries 30
 cookie size 8
```

Konfigurasi parameter pseudowire menggunakan nama yang sama dengan nama pseudowire pada LNS 1 yaitu "test".

```
pseudowire-class test
 encapsulation l2tpv3
 protocol l2tpv3 test
 ip local interface Loopback1
```

Konfigurasi IPSec menggunakan “cisco” sebagi kunci komunikasinya yaitu sama dengan kunci kriptography pada LNS 1.

```
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
```

Setelah itu dilanjutkan dengan konfigurasi transform set untuk mendefinisikan alamat ip tujuan *tunneling* yang akan dilakukan oleh IPSec.

```
crypto ipsec transform-set vpn esp-3des esp-sha-hmac
!
crypto map vpn 10 ipsec-isakmp
 set peer 20.1.1.2
 set transform-set vpn
 match address vpn
```

Konfigurasi *interface loopback1*, *interface fastethernet0/0,* dan *interface fastethernet0/1*adalah sebagai berikut.

```
interface Loopback1
 ip address 10.1.4.1 255.255.255.0
 no shutdown
interface FastEthernet0/0
 ip address 30.1.1.2 255.255.255.0
 no shutdown
 duplex auto
 speed auto
 crypto map vpn
```

Pada konfigurasi *Fast Ethernet 0/1* terdapat konfigurasi “xconnect 10.1.1.1 100 encapsulation l2tpv3 pw-class test” .

```
interface FastEthernet0/1
 description LAN
 no ip address
 no shutdown
```

```
 duplex auto
 speed auto
 xconnect 10.1.1.1 100 encapsulation l2tpv3 pw-class test
```

Konfigurasi *route* adalah sebagai berikut.

```
ip route 0.0.0.0 0.0.0.0 30.1.1.1
```

Konfigurasi traffic acces list sebagai berikut.

```
ip access-list extended vpn
 permit ip host 10.1.4.1 host 10.1.1.1
```

Skrip lengkap konfigurasi pada *router 2* terlampir.

3.2.5.3 Konfigurasi ISP 1

ISP1 berfungsi menentukan *routing* dari LNS ke ISP2. Konfigurasi pada ISP1 dilakukan secara manual. Konfigurasi *interface* dan routing yang diberikan adalah sebagai berikut.

Konfigurasi pada *Interface Fast Ethernet 0/0* adalah sebagai berikut.

```
interface FastEthernet0/0
  ip address 20.1.1.1 255.255.255.0
  duplex auto
  speed auto
  no shutdown
```

Konfigurasi pada *Interface Fast Ethernet 0/1* adalah sebagai berikut.

```
interface FastEthernet0/1
  ip address 40.1.1.1 255.255.255.0
  duplex auto
  speed auto
  no shutdown
```

Konfigurasi *routing* dilakukan untuk mengarahkan agar LNS1 dapat berkomunikasi dengan ISP2

```
ip route 0.0.0.0 0.0.0.0 10.1.1.2
ip route 0.0.0.0 0.0.0.0 40.1.1.2
```

Skrip lengkap konfigurasi pada ISP 1 terlampir.

3.2.5.4 Konfigurasi ISP 2

Konfigurasi ISP 2 tidak jauh berbeda dengan konfigurasi pada ISP 1. Konfiguasi *Interface Fast Ethernet 0/0* adalah sebagai berikut:

```
interface FastEthernet0/0
 ip address 30.1.1.1 255.255.255.0
 duplex auto
 speed auto
 no shutdown
```

Konfigurasi *Interface Fast Ethernet 0/1*

```
interface FastEthernet0/1
 ip address 40.1.1.2 255.255.255.0
 duplex auto
 speed auto
 no shutwown
```

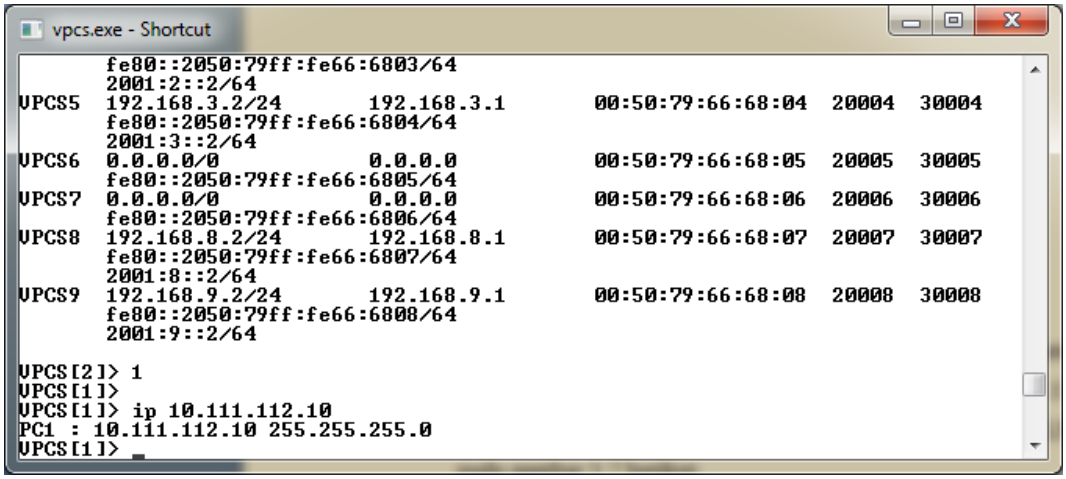
Konfigurasi *Routing*

```
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 0.0.0.0 0.0.0.0 40.1.1.1
```

Skrip konfigurasi pada ISP 2 secara lengkap terlampir.

3.2.5.5 Konfigurasi PC Client

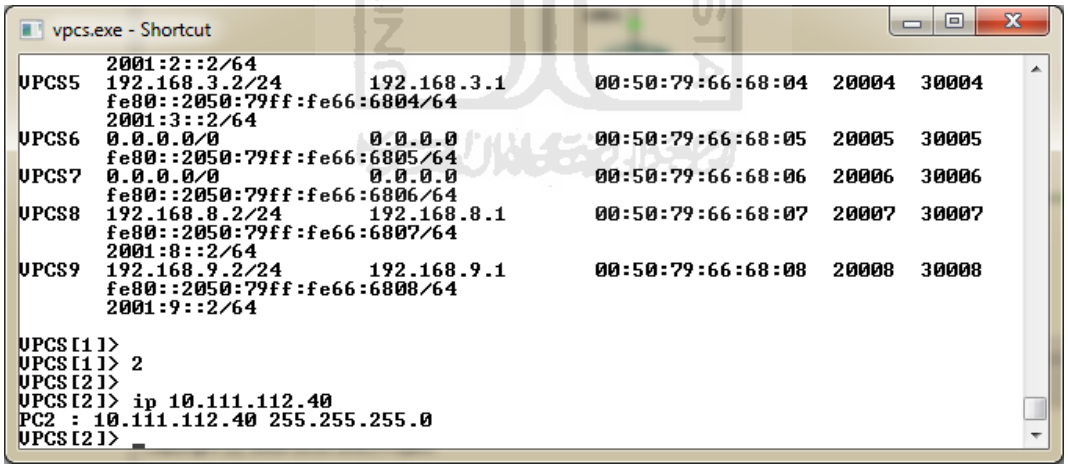
Client user diimplementasikan sebagai cloud yang telah terintegrasikan dengan VPCS, dengan cara menyamakan nomor *local* port dan *remote* portnya. *Client* berperan sebagai user yang terhubung ke LNS1 atau LNS2. *Client* menggunakan VPCS yang dapat melakukan fungsi dasar sebuah PC. Konfigurasi yang dapat dilakukan adalah konfigurasi alamat IP dan gateway sebagai berikut.



Gambar 3. 6 Konfigurasi IP pada PC1

Pada gambar 3.6 ditunjukkan penentuan alamat IP dan gateway pada PC1. PC1 memiliki alamat IP 10.111.112.10 dan gateway 10.111.112.1.

Selanjutnya adalah konfigurasi PC2 yang terhubung ke LNS2, dapat ilihat pada gambar 3.7 berikut.



Gambar 3. 7 Konfigurasi IP pada PC2

Pada gambar 3.7 dapat dilihat bahwa PC2 diberi alamat IP 10.111.112.40 dengan gateway 10.111.112.1 .

3.3 Rencana Pengujian

Rencana pengujian yang akan dilakukan dibagi dalam beberapa tahapan, yang pertama yaitu melakukan cek status L2TP pada kedua LNS untuk mengetahui apakah skenario *tunneling* L2TP telah terbentuk dengan sempurna. Dilanjutkan dengan melakukan cek status protokol IPSec yang telah dikonfigurasikan. Apabila skenario L2TPv3 over IPSec telah berjalan, dapat dibuktikan dengan melakukan uji koneksi L2TPv3 dari PC1 ke PC2.

Setelah terjalin koneksi dari PC1 ke PC2 dengan topologi seperti yang dapat dilihat pada gambar 3.5, itu artinya skenario *tunneling* L2TPv3 over IPSec telah berjalan sesuai dengan yang direncanakan. Tahapan terakhir yaitu melakukan uji keamanan *tunneling* protokol L2TPv3 over IPSec dengan melakukan *capture* menggunakan *software* Wireshark. *Capture* disini sebagai *sniff* yang akan membuktikan apakah protokol IPSec bekerja secara optimal. Titik keberhasilan terlihat pada perbedaan hasil *capture* antara topologi yang menggunakan *tunneling* L2TPv3 tanpa IPSec dengan topologi yang menggunakan *tunneling* L2TPv3 yang dikombinasikan dengan IPSec. Pada *capture* L2TPv3 over IPSec, tidak akan terlihat informasi-informasi seperti protokol *tunneling, id tunnel, dan hello paket*, karena telah terbungkus oleh protokol ESP yang merupakan bagian dari keamanan yang disediakan oleh protokol IPSec.

BAB IV
HASIL DAN PEMBAHASAN

4.1 Hasil Pengujian

4.1.1 Hasil Pengujian Server (LNS)

Pengujian pada server diawali dengan melakukan verifikasi terhadap konfigurasi yang telah dilakukan, hal ini ditujukan untuk melihat apakah protokol L2TP dan IPSec berjalan dengan semestinya.

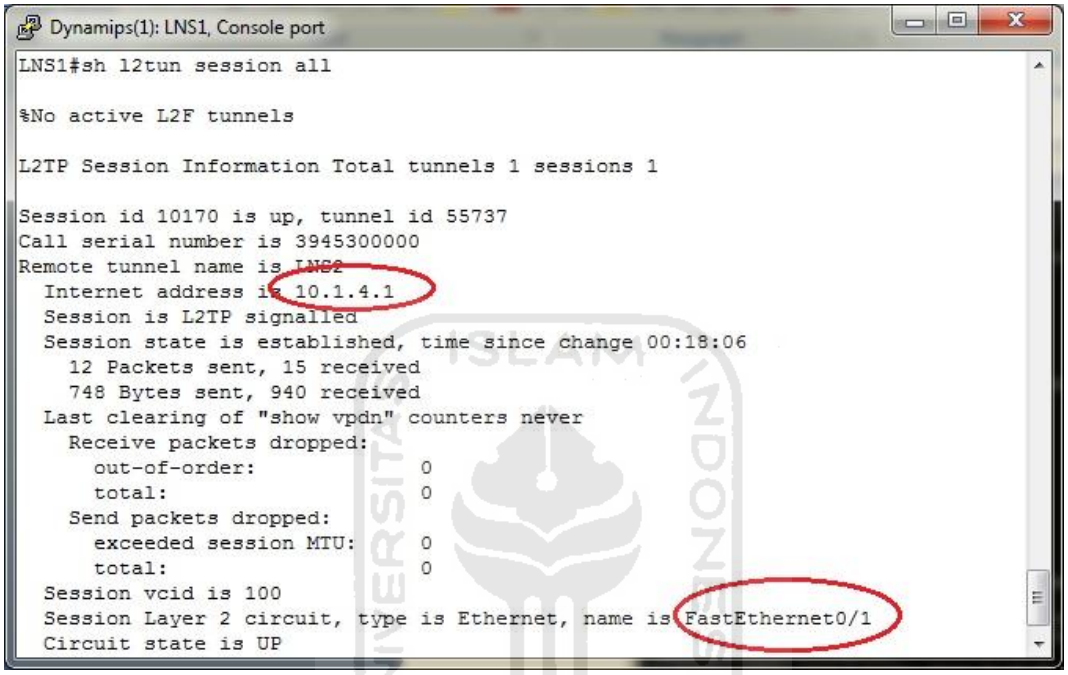
4.1.1.1 Melihat Status L2TP

Pengecekan status *tunnel* L2TP dapat dilakuakan dengan perintah "#show l2tun". Dapat dilihat pada gambar 4.1 berikut .

Gambar 4.1 Tampilan Informasi Layer 2 Tunneling

Pada gambar 4.1 dapat dilihat informasi tunneling menggunakan protokol L2TP yang mengarah ke alamat IP 10.1.4.1. Dalam informasi ini juga dapat dilihat nama dari group dari *l2tp-class* yakni "test". Dua protokol *tunneling* lain L2F dan PPTP statusnya adalah *no active tunnel.*

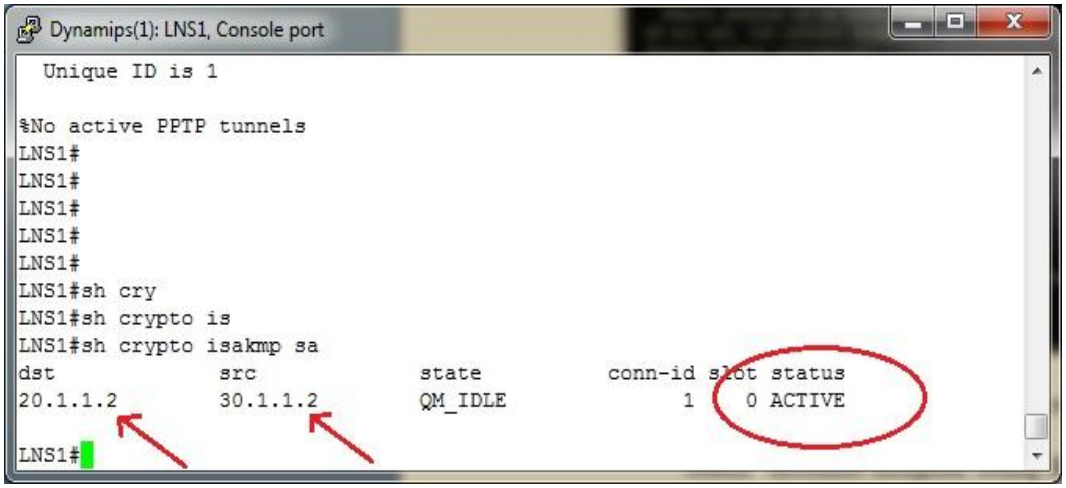
Untuk tampilan informasi sesi L2TP secara lengkap dapat dilihat dengan menggunakan perintah "#show l2tun session all". Perintah ini juga menampilkan alamat tujuan, jumlah paket yang di kirim dan tersampaikan, dan *interface* yang melakukan koneksi L2TP. Dapat dilihat pada gambar 4.2 berikut.



Gambar 4.2 Informasi Protokol Semua Sesi L2TPv3

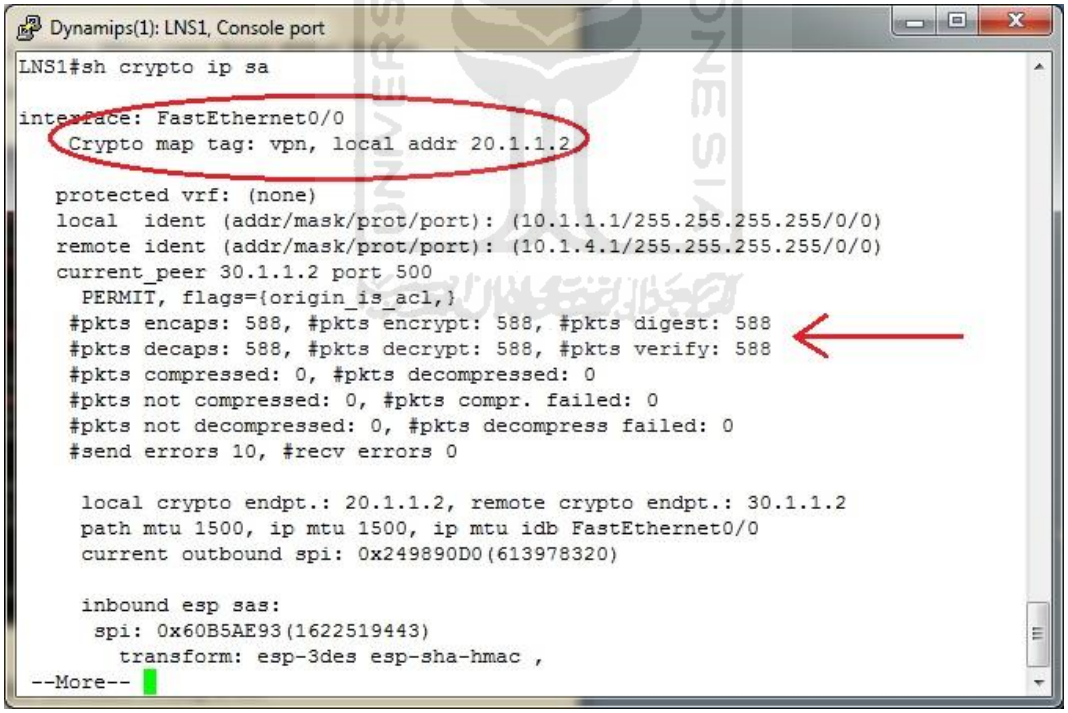
4.1.1.2 Pengujian Status IPSec

Apabila skema IPSec yang mengenkapsulasi paket L2TP telah berjalan secara optimal, informasi status kunci keamanan IKE menuju tujuan dapat dilihat dengan perintah "#show crypto isakmp sa". Dapat dilihat status IKE dari chanel *source* menuju *destination* sudah aktif atau belum.

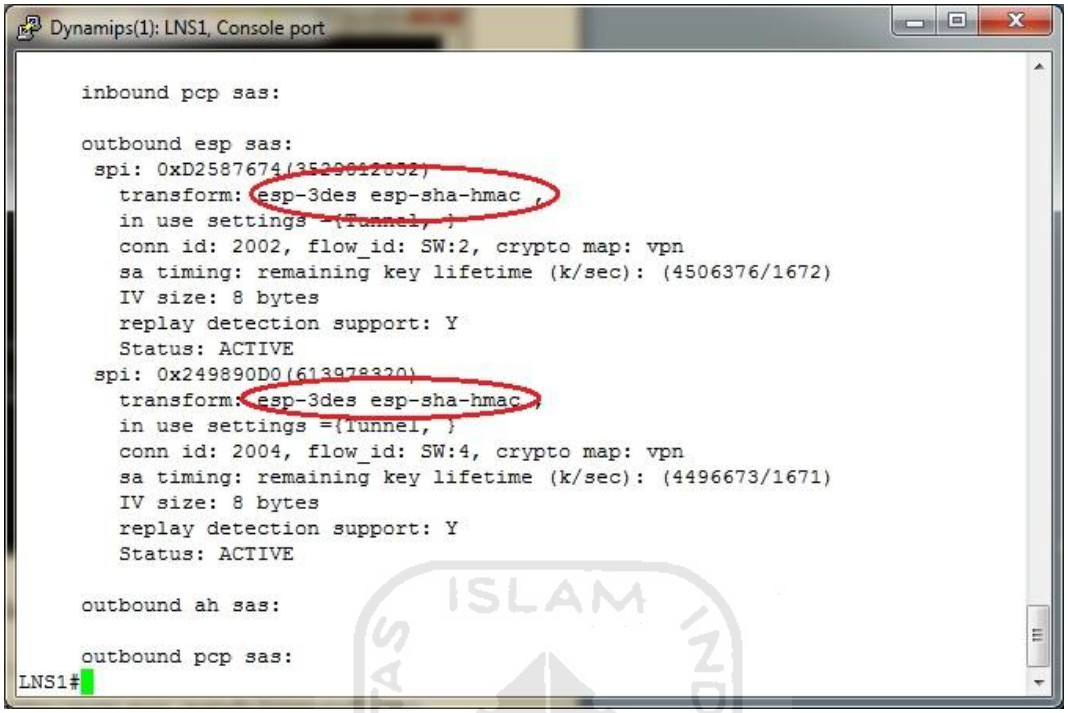


Gambar 4.3 Tampilan Channel IKE Aktif

Semua informasi mengenai setting IPSec yang dapat dilihat dengan memberikan perintah "#show crytpo ipsec sa".



Gambar 4.4 Tampilan Informasi Setting IPSec

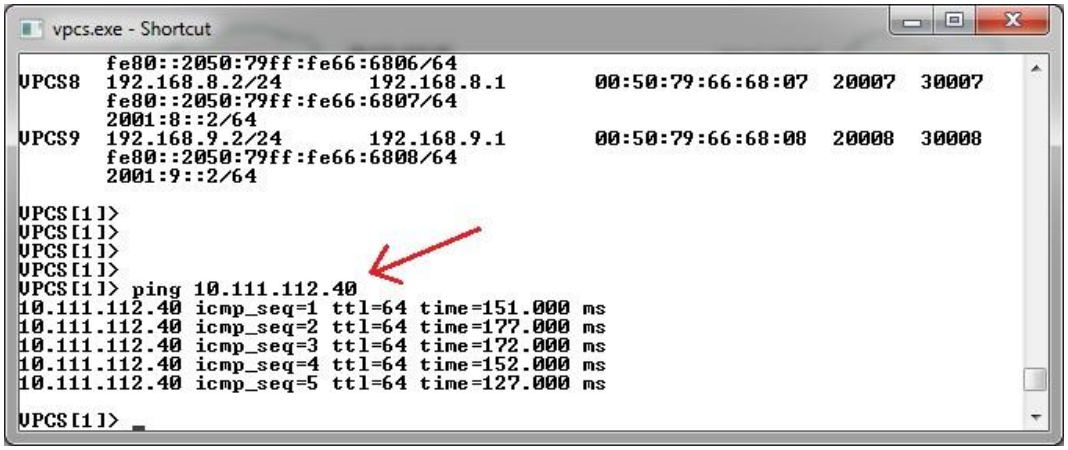


Gambar 4.5 Tampilan Informasi Setting IPSec

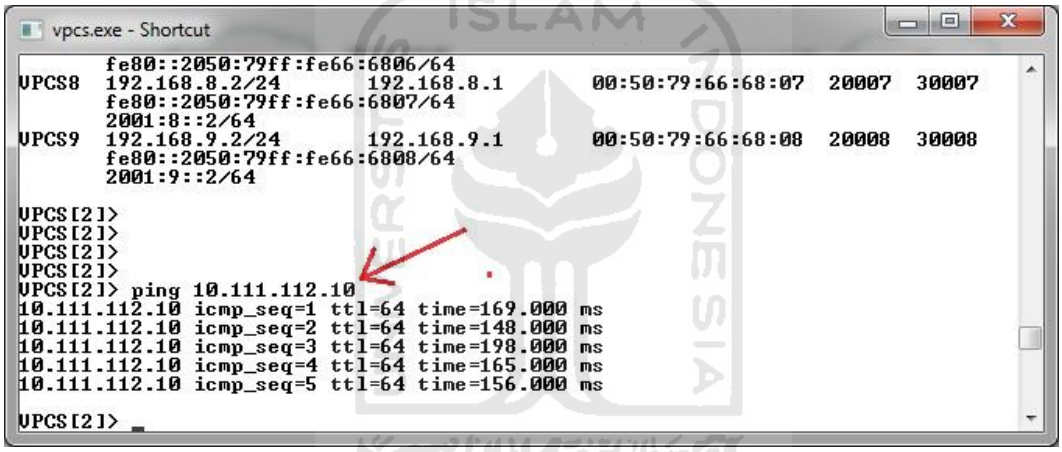
Gambar 4.4 dan gambar 4.5 memperlihatkan hasil konfigurasi IPSec. Terdapat beberapa informasi seperti nama *crypto map*, metode kriptografi yang dipakai dan informasi mengenai banyaknya paket yang dapat dienkripsi dan terdeskripsi dari semua paket data yang dikirimkan.

4.1.2 Hasil Pengujian Client

Pengujian pada sisi *client* diawali dengan mengecek keadaan atau status komputer *client* untuk menunjukkan bahwa *client* yang berada pada jaringan yang berbeda dapat saling berkomunikasi melalui tunnel L2TPv3 .



Gambar 4. 6 Komunikasi ICMP dari PC1 ke PC2



Gambar 4. 7 Komunikasi ICMP dari PC2 ke PC1

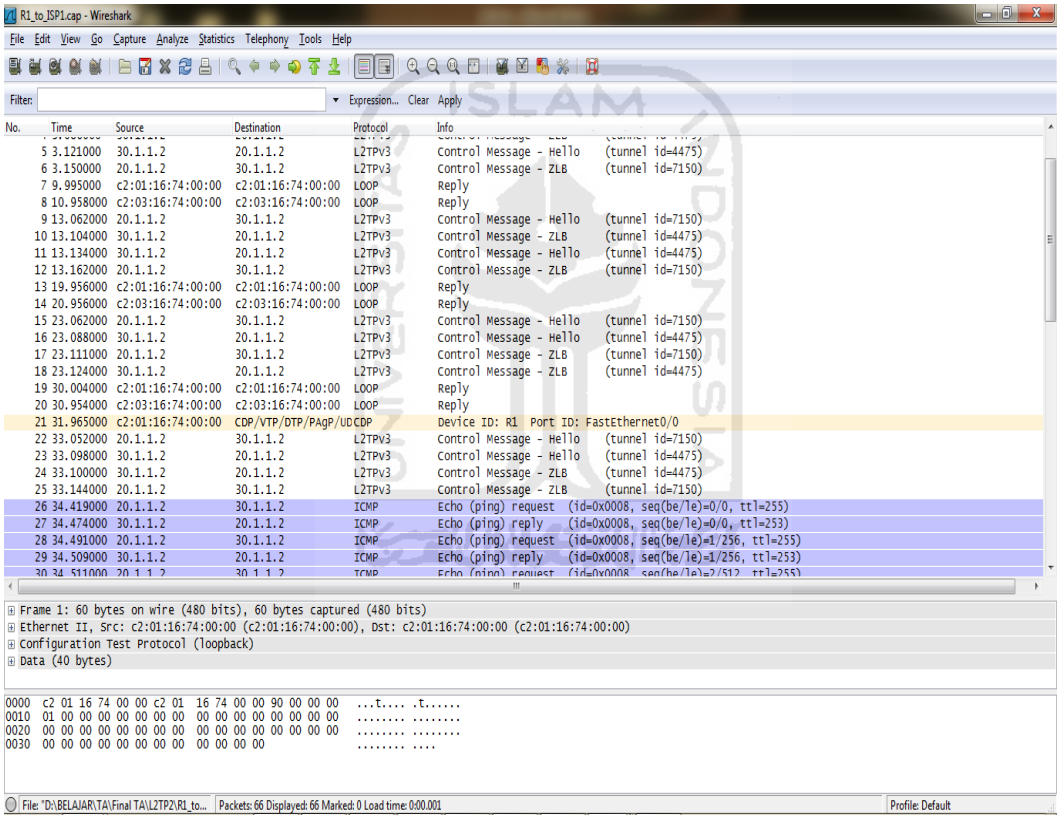
Dari gambar 4.6 dan gambar 4.7 dapat dilihat bahwa tunnel L2TPv3 dari LNS1 menuju LNS2 telah berhasil dibentuk. Hal ini ditandai dengan komunikasi data yang dapat dilakukan dari PC1 dan PC2 dan sebaliknya.

Untuk tampilan komunikasi L2TPv3 secara lengkap terlampir.

4.1.3 Hasil Pengujian Keamanan

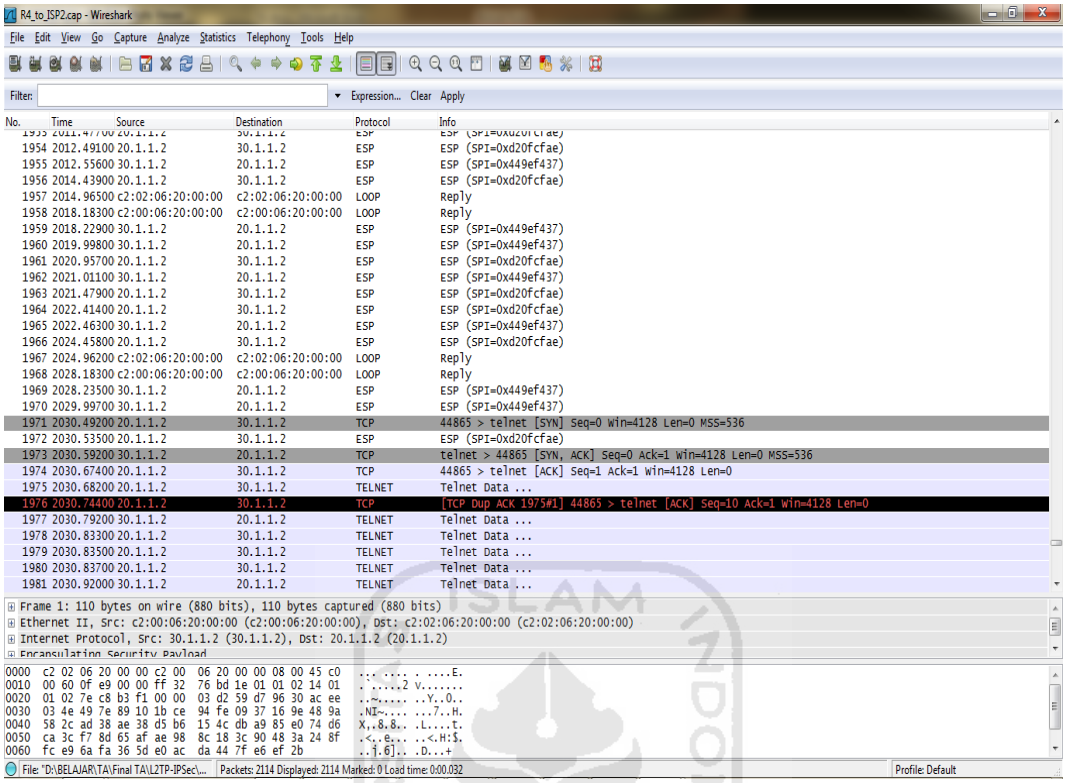
Skema uji keamanan dilakuakn menggunakan *software* wireshark untuk melakukan *sniff*. Pengujian ini bertujuan melihat perbedaan tingkat keamanan L2TP sebelum menggunakan IPSec dan L2TP yang telah di kombinasikan dengan teknologi IPSec.

Sebelum menggunakan IPSec, hasil *sniffing* pada jalur antara LNS1 dan ISP1 akan menampilkan tunnel L2TP yang belum terlindungi. Disini terlihat jelas paket masih belum di enkasulasi karena dapat diketahui jenis *tunnel* dan id *tunnel* yang digunakan.

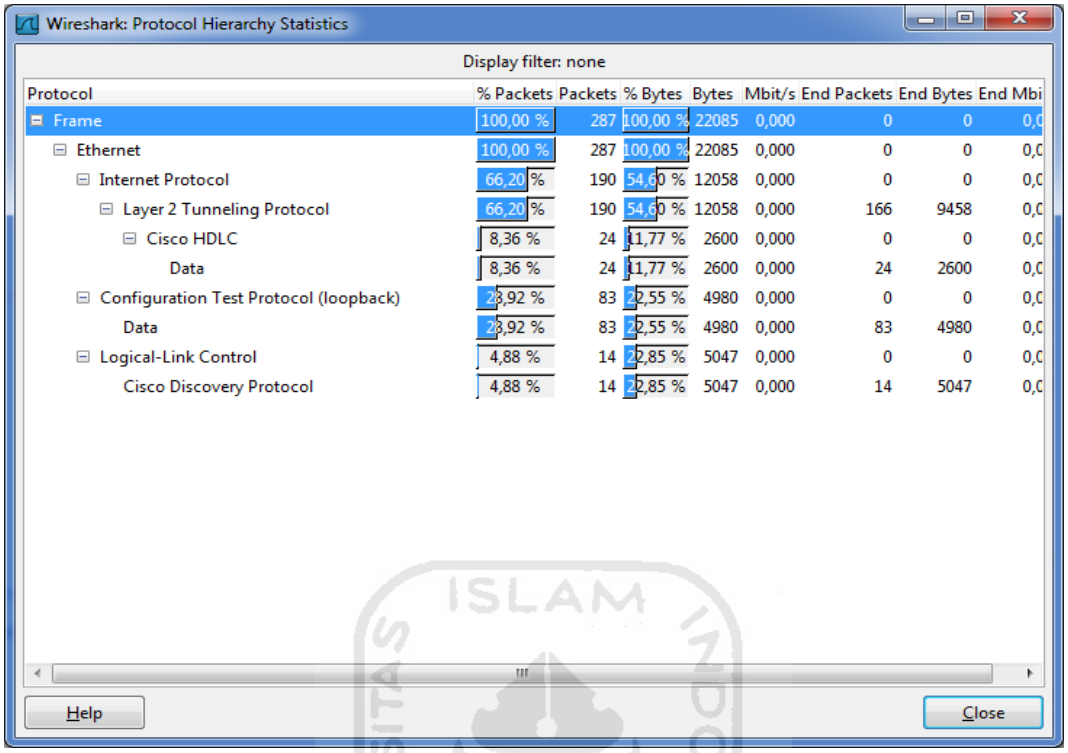


Gambar 4. 8 Capture L2TPv3 dari LNS1 ke ISP1

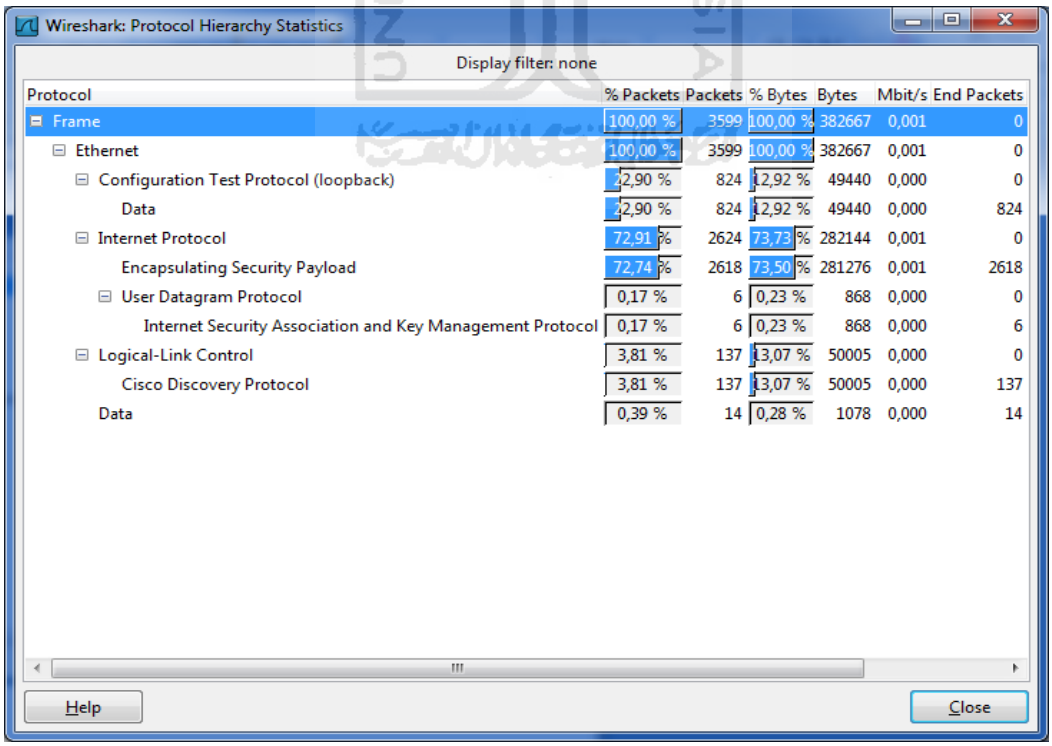
Setelah *tunnel* L2TPv3 dan IPSec terbentuk, paket data yang dilewatkan ke dalam *tunnel* dalam keadaan terenkripsi dan terlindungi, sehingga jenis paketnya tidak dapat terlihat oleh *sniffer* seperti terlihat pada gambar 4.9.



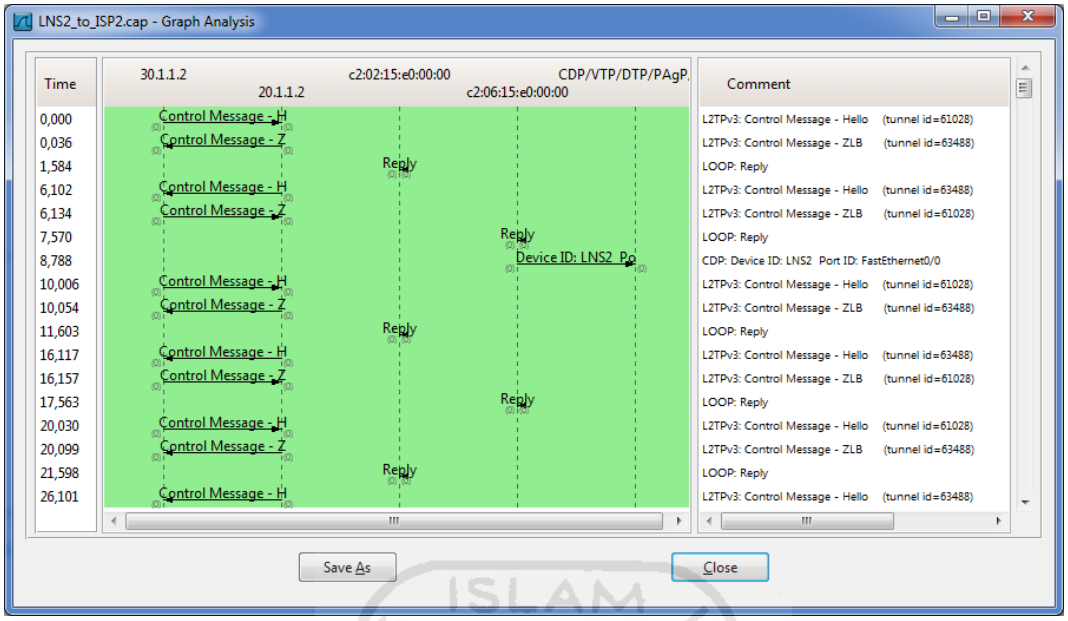
Gambar 4. 9 Capture L2TPv3 over IPSec dari LNS1 ke ISP1



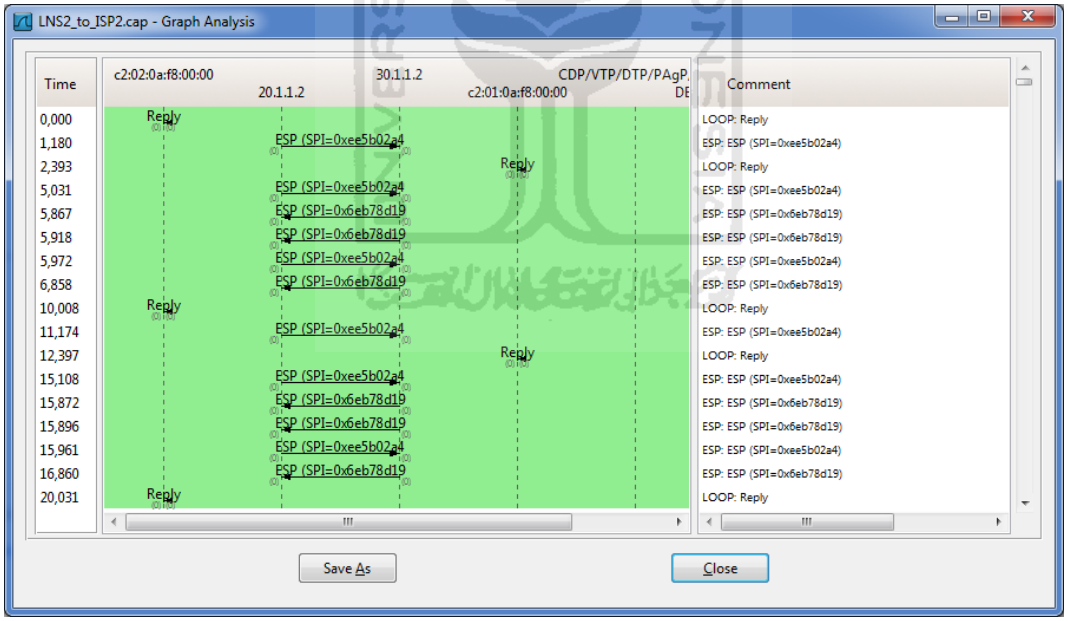
Gambar 4. 10 Statistik hirarki L2TPv3 (LNS2 to ISP2)



Gambar 4. 11 Satistik hirarki L2TPv3 Over IPSec (LNS2 to ISP2)



Gambar 4. 12 Aliran grafik L2TPv3 (LNS2 to ISP2)



Gambar 4. 13 Aliran grafik L2TPv3 Over IPSec (LNS2 to ISP2)

Untuk tampilan hasil *sniffing* lain dengan wireshark terlampir.

4.2 Pembahasan Hasil Pengujian

4.2.1 Komunikasi Paket Data

Setelah melihat hasil pengujian dari sisi *client* dan LNS, menunjukkan bahwa skenario L2TPv3 over IPSec telah berjalan sesuai dengan yang direncanakan. Kemudian dapat dilakukan analisis perbandingan parameter jumlah hop (lompatan), ttl, dan waktu tempuh antara sebelum menggunakan VPN, setelah menggunakan VPN dengan L2TP dan setelah menggunakan VPN dengan L2TP Over IPSec. Perbandingan komunkasi data dapat dilihat dari tabel 4.1 berikut.

Tabel 4.1 Perbandingan Komunikasi Paket data

Parameter	**Sebelum VPN**	**Sesudah VPN dengan L2TP**	**Sesduah VPN dengan L2TP Over IPSec**
Jumlah Hop	3	1	1
TTL	61	64	64
Waktu Tempuh / Time (Rata-rata dari 10 kali ICMP)	30.000 ms	57.000 ms	155.000 ms

Dari tabel 4.1, perbandingan jelas terlihat dari jumlah hop sebelum menggunakan vpn dan setelah menggunakan VPN. Sebelum menggunakan VPN, secara *logic client1* harus melalui 8 hop untuk menuju *client2*. Kemudian setelah menggunakan VPN *client1* hanya mengenali *client2* tanpa menghiraukan berapa router yang dilewati untuk menuju ke *client2*. Perbandingan selanjutnya terlihat pada jumlah *time to life* (ttl) sebelum mnggunakan VPN dan sesudah menggunakan VPN, panjang ttl akan di kalkulasikan pada jumlah hop yang dilewati dengan kalkulasi ttl-1 setiap melewati 1 hop. Berbeda dengan perbandingan waktu tempuh dari *client1* menuju *client2*, setelah menggunakan

VPN baik hanya dengan L2TP mauapun setelah di tambah IPSec, waktu tempuh akan lebih lama dibandingkan sebelum menggunakan VPN. Hal ini dikarenakan VPN harus melalui proses enkapsulasi yang tentunya menambah waktu persiapan untuk pengiriman paket. Hal itu pula yang menyebabkan setelah diberi IPSec waktu tempuh akan menjadi lebih lama dibanding dengan hanya menggunakan *tunnel* L2TP.

4.2.2 Keamanan Paket Data

Untuk melihat apakah kedua protokol tersebut sudah berjalan optimal, dilakuakan pengujian keamanan dengan melakukan *sniff* menggunakan *capture* Wireshark. Pada gambar 4.8 dan gambar 4.9, dapat terlihat perbedaan antara L2TPv3 yang berdiri sendiri dan L2TPv3 yang telah dikombinasikan dengan enkapsulasi IPSec.Tabel 4.1 menunjukkan pe perbandingan enkapsulasi paket, penggunaaan port UDP dan pertukaran *message control* sebelum dan sesudah menggunakan L2TP Over IPSec.

Tabel 4.2 Pebandingan keamanan paket data

Parameter	**L2TP**	**L2TP Over IPsec**	**Ket**
Enkapsulasi	-Ada -Terlihat	-Ada -Tidak terlihat	L2TP Over IPSec meng enkapasulasi kembali Paket L2TP dengan protokol ESP.
Enkripsi	Tidak ada	Ada	Enkripsi paket oleh protokol ESP pada L2TP over IPSec.
User Datagram Protocol	Tidak ada	Ada	L2TP Ove IPSec Meng-gunakan port UDP un tuk pertukaran IKE
Message Control	Terlihat	Tidak terlihat	Message control seperti hello, ZLB dan id-tunnel terenkripsi oleh ESP

Sebelum menggunakan IPSec, paket L2TP yang dikirimkan masih terlihat oleh *sniffer* pada *capture*, dan setelah menggunakan IPSec, paket L2TPv3 dienkapsulasi dan dienkripsi oleh protokol ESP sehingga tidak terlihat oleh *sniffer*. IPSec menggunakan port *User Datagram Protocol* (UDP) untuk melewatakan IKE sebagai kunci keamanan komunikasi data. Kemudian *message contcrol* seperti hello, ZLB dan id-tunnel pada L2TP over IPSec telah di enkripsi oleh protokol ESP.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah melakukan implementasi dan pengujian, dapat diambil kesimpulan sebagai berikut.

1. Untuk menyediakan komunikasi yang aman melalui jaringan publik, termasuk Internet, L2TP pada layer 2 dapat dikombinasikan dengan IPSec pada layer 3. IPSec akan memberi layanan enkripsi dan autentikasi.
2. L2TPv3 dapat digunakan untuk implementasi site-to-site VPN dengan model topologi LNS-LNS.
3. IPSec merupakan protokol keamanan pada *network layer* yang mengenkapsulasi paket IP dan melakukan enkripsi pada paket tersebut, sehingga apabila terjadi penyadapan data oleh pihak ketiga, data asli tidak dapat terlihat
4. Untuk implementasi site-to-site VPN antara korporat ke korporat, L2TPv3 over IPSec dapat menjadi solusi karena terbukti mampu menjalankan fungsi *tunnel* secara optimal dan keamanan data terlindungi.

5.2 Saran

Dari hasil pengujian dan implementasi yang telah dilakukan, terdapat beberapa saran yang perlu disampaikan yaitu:

1. Supaya dilakukan implemantasi lain seperti *remote acces* VPN dengan protokol L2TPv3 over IPSec supaya dapat dilihat kinerja protokol AH (*Authentication Header*) pada saat melakukan proses dial-up.
2. Supaya dapat dikembangkan pengujian dengan metode lain bukan hanya *sniffing* (penyadapan data).

DAFTAR PUSTAKA

[ASF07] Asfihandi, Yulian Eka. 2007. "*Implementasi Remote Acces Virtual Private Network (VPN) pada Linux dengan client Windows*". Jogjakarta : Perpustakaan FMIPA UGM

[CISCO] "*L2TPv3: Layer-2 Tunnel Protocol Version 3*". Diakses dar http://www.cisco.com/

[MAR10] Martin, W. Murhammer. "*Layer 2 Tunneling Protocol (L2TP)*". international Technical Support Center. Diakses dari http://www.ibm.com/ pada tanggal 2 agustus 2010

[NKC10] Nemo of Kecoak Elektronik, "*Fun With the IP Security Protocol*". Diakses dari http://www.kecoak-elektronik.net pada tanggal 17 july 2010.

[PAS04] Pasaribu, Novi Theresia BR. 2004. "*Protokol L2TP*".Bandung :Teknik Elektro - Institut Teknologi Bandung. Diakses melalui http://www.look-pdf.com/37034940-PROTOKOL%20L2TP.html

[PUR00] Purbo, Onno W. 2000. "*Apa Bedanya Internet,Intranet, dan Ekstranet*".
Diakses dari http://www.deptan.go.id/pusdatin/admin/RB/Internet/ pada 2 agustus 2010

[RFC2661] Townsky, W and Network Working Group. " *Layer Two Tunneling Protocol (L2TP)* ".
Diakses dari http://www.faqs.org/rfcs/rfc2661.html

[RFC3931] Townsky, W and Network Working Group. "*Layer Two Tunneling Protocol – Version 3 (L2TPv3)*".
Diakses dari http://www.faqs.org/rfcs/rfc3931.html

[SAN04] Sanny, Muhammad Rusdy. 2004.*"Keamanan Jaringan Virtual Private Network".*
Diakses dari http://www.scribd.com/doc/41147053/Keamanan-Jaringan-Virtual-Private-Network pada tanggal 25 juli 2010