BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan chip silikon yang dimulai sejak tahun 1949, kini sudah berkembang dengan pesat. Hal ini dapat dilihat dari perkembangan teknologi komputer saat ini, yang menggunakan berbagai macam chip silikon pada perangkat sirkuit terintegrasi. Tidak hanya pada dunia komputer saja, perkembangan ini juga merambah bidang komunikasi, dan industri. Ditandai dengan adanya revolusi industri, pekerjaan manusia sangat terbantu dengan adanya mesin-mesin industri yang tidak dapat terlepas dari chip silikon sebagai pengendalinya. Sedangkan di dunia telekomunikasi saat ini, sangat memungkinkan bagi seseorang untuk memiliki telepon dan komputer dalam satu perangkat yang sama.

Berkembangnya dunia komunikasi ini, juga membawa perkembangan pada dunia yang ssekarang mengenal Internet. Internet pada awalnya merupakan sebuah proyek ARPA yang digawangi oleh Departemen Pertahanan Amerika Serikat pada tahun 1969, dengan nama ARPANET. Pada proyek ini, mereka mendemonstrasikan bagaimana dengan hardware dan software komputer yang berbasis UNIX, user bisa melakukan komunikasi dalam jarak yang tidak terhingga melalui saluran telepon. Proyek ARPANET merancang bentuk jaringan, kehandalan, seberapa besar informasi dapat dipindahkan, dan akhirnya semua standar yang mereka tentukan menjadi cikal bakal pembangunan protokol baru yang sekarang dikenal sebagai TCP/IP (*Transmission Control Protocol/Internet Protocol*). Tujuan awal dibangunnya proyek itu adalah untuk keperluan militer. Pada saat itu Departemen Pertahanan Amerika Serikat (US Department of Defense) membuat sistem jaringan komputer yang tersebar dengan menghubungkan komputer di daerah-daerah vital untuk mengatasi masalah bila terjadi serangan nuklir dan untuk menghindari terjadinya informasi terpusat, yang apabila terjadi perang dapat mudah dihancurkan.

Pada perkembangannya hingga saat ini, sudah muncul beberapa perangkat yang berguna untuk menghubungkan jaringan. Antara lain *Hub*, *Switch*, dan *Router*. Switch berfungsi untuk menghubungkan beberapa perangkat komputer menjadi satu jaringan. Sedangkan Router bertugas untuk menghubungkan beberapa jaringan kecil, menjadi sebuah jaringan besar yang merupakan akar dari Internet. Hub sendiri yang merupakan pendahulu dari switch, sudah mulai ditinggalkan karena penggunaannya yang kurang efisien dibandingkan switch.

Internet, tidak bisa lepas dari peran router. Router bekerja pada *Layer* 3 OSI, yaitu *Network Layer*. Tugas utama router adalah memisahkan jaringan. Selain itu router juga bertugas mengarahkan, kemana paket data harus diteruskan. Penerusan paket data ini, dilakukan berdasarkan table *routing* yang dimiliki oleh router yang bersangkutan. Hanya saja, terdapat beberapa macam metode pembentukan tabel routing. Antara lain *Static Routing*, RIP, OSPF, dan EIGRP.

Fungsi Router sebagai VPN (Virtual Private Network), memungkinkan dua jaringan yang letaknya berjauhan, namun masih terjangkau oleh Internet, untuk terhubung secara privat. VPN merupakan suatu bentuk *private* Internet yang melalui *public network* (Internet), dengan menekankan pada keamanan data dan akses global melalui Internet. Hubungan ini dibangun melalui suatu *tunnel* (terowongan) virtual antara 2 node. Dengan kata lain, VPN mampu membentuk jaringan local, dengan menggunakan IP public yang dimiliki oleh dua jaringan yang akan berhubungan, tanpa mengesampingkan keamanan data.

Dengan adanya fungsi VPN ini, akan sangat memungkinkan bagi sebuah perusahaan di pusat yang memiliki cabang, untuk terhubung pada suatu jaringan lokal. Sehingga *server* data, dapat terpusat di kantor pusat, tanpa harus membuat server data lagi pada kantor cabang. Fungsi utama dari VPN adalah, membuat jaringan privat melalui Internet.

1.2. Tujuan

Tujuan dari tugas akhir ini adalah:

- Mengimplementasikan VPN untuk membentuk jaringan pribadi pada *Wide Area Network* dengan menggunakan Router Cisco 1841

- Menganalisa sistem keamanan dan kinerja antara jaringan yang menggunakan VPN dengan jaringan tanpa VPN.

1.3. Teori Penunjang

Berikut ini merupakan beberapa teori penunjang yang dibutuhkan dalam pembuatan tugas akhir ini:

1. Teori Dasar Jaringan Komputer

   Teori ini digunakan sebagai dasar pembangunan sebuah jaringan dan diperlukan dalam melakukan proses pengiriman data dari suatu tempat ketempat lain. Teori ini berisi tentang dasar-dasar jaringan komputer, seperti 7 layer OSI dan alamat IP. Hal-hal mendasar seperti *Subnetting* atau pembagian jaringan juga dijelaskan pada teori ini.

2. Router dan *Routing Protocol*

   Pengetahuan tentang router dan routing protokol diperlukan untuk menghubungkan dua jaringan atau lebih, supaya dapat berkomunikasi satu sama lain. Adapun routing protokol yang ada, antara lain static routing, RIP dan OSPF. Routing protocol berfungsi untuk membentuk routing table untuk mengarahkan paket data menuju network tujuan.

3. Wide Area Network

   Wide Area Network merupakan jaringan komputer berukuran luas. Sering kali disebut dengan Internet. WAN di sini akan berfungsi sebagai media dalam pembentukan jaringan virtual.

4. Virtual Private Network

   Virtual Private Network atau VPN adalah konsep yang digunakan untuk membuat jaringan lokal secara virtual melalui WAN dengan melakukan beberapa proses seperti Enkripsi, Enkapsulasi, dan Tunneling. Pada tugas akhir ini, yang akan dibahas secara mendalam adalah VPN dengan menggunakan Router Cisco 1841.

5. *Network Security*

   Teori keamanan jaringan, yang berguna untuk mengamankan pengiriman atau transfer data. Adapun beberapa di antaranya yaitu MD5 dan SHA.

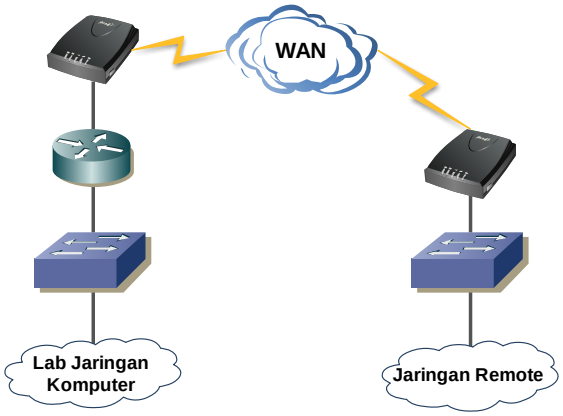
Metode-metode tersebut merubah data-data yang akan dikirimkan menjadi kode-kode terselubung, yang kemudian akan diterjemahkan oleh resipien atau penerima, sehingga pihak-pihak yang tidak berkepentingan tidak dapat mengetahui isi data yang dikirimkan.

1.4. Ruang Lingkup

Ruang lingkup yang akan dibahas pada tugas akhir ini adalah sebagai berikut:

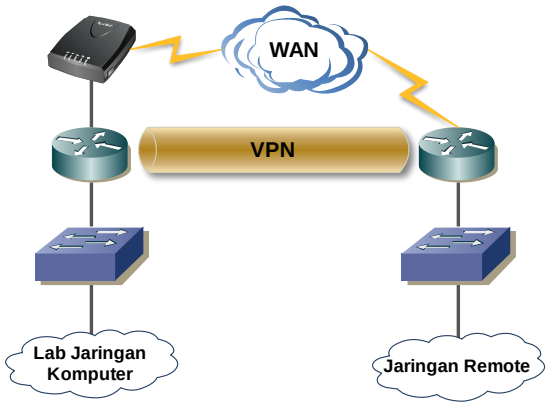
1. Arsitektur sistem

   Sistem jaringan akan dibuat dengan menggunakan dua buah router Cisco 1841 pada masing-masing ujungnya, di mana di antara kedua ujung tersebut terhubung pada WAN atau Internet. Pada jaringan yang nyata, jaringan privat dari masing-masing ujung dapat bermacam-macam, namu untuk percobaan ini, digunakan masing-masing sebuah switch dan dua buah komputer pada kedua ujungnya.



Gambar 1.1
Jaringan Awal

Pada percobaan skala kecil, WAN akan diemulasikan dengan WAN tiruan berupa pemasangan beberapa router yang terhubung satu sama lain dan mampu berkomunikasi satu sama lain menggunakan tabel routing. Dan untuk percobaan skala besar, akan dihubungkan menuju ke jaringan Internet menggunakan dua buah ISP yang berbeda.



Gambar 1.2
Tunneling VPN

Pada implementasi VPN, yang terjadi adalah terbentuknya jaringan virtual, atau yang digambarkan seperti tunnel yang menghubungkan secara langsung dua titik yang berjauhan dan terhubung pada WAN menjadi sebuah jaringan privat. Pada tunnel ini, data mengalami:

1) Encapsulation

   Data yang dikirimkan dibungkus dengan menggunakan data-data yang lain. Adapun data-data tersebut berisi informasi-informasi guna membuka bungkusan tersebut. Adapun informasi-informasi tersebut, antara lain:

   - Security Parameters Index
   - Sequence Number
   - Payload data
   - Padding
   - Pad Length
   - Next Header
   - Integrity Check Value

   Bungkusan tersebut akan dibuka oleh penerima dengan menggunakan informasi-informasi yang disisipkan pada data yang sudah terenkapsulasi sebelumnya.

2) Encryption

Data yang dikirim dikodekan menjadi sebuah kode rahasia sesuai perjanjian kedua ujung, pengirim dan penerima. Sebelum pengiriman, data mengalami proses enkripsi, dan setelah diterima, data mengalami proses dekripsi. Beberapa metode enkripsi yang sering digunakan adalah DES, 3DES, dan AES.

Untuk mendukung studi analisa ini, akan dilakukan studi kasus mengenai implementasi VPN menggunakan Router Cisco 1841 yang menghubungkan Laboratorium Jaringan STTS, dengan jaringan di lokasi lain dengan menggunakan media jaringan yang disediakan oleh ISP. Sehingga efek VPN melalui WAN dapat dianalisa.

2. Batasan Sistem

Berikut ini beberapa batasan dalam sistem yang akan dianalisa:

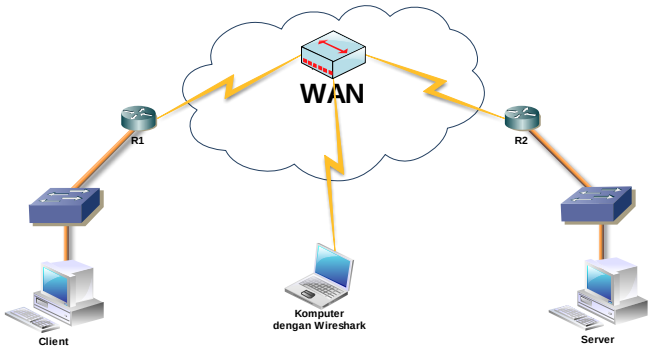
1) Router yang digunakan adalah Cisco 1841 dengan Sistem Operasi "c1841-advsecurityk9-mz.124-23" yang akan digunakan sebagai penghubung antara dua jaringan
2) Protokol keamanan yang akan digunakan adalah *Internet Protocol Security* (IPsec)
3) Protokol kriptorafi yang akan digunakan adalah *Internet Security Association and Key Management Protocol* (ISAKMP)

3. Analisa Keamanan

Keamanan merupakan hal yang terpenting pada pembahasan tugas akhir ini. Sesuai dengan namanya, Virtual Private Network, atau jaringan pribadi virtual, menjanjikan sebuah jaringan privat, yang melalui jaringan umum secara virtual. Jaringan umum, dalam konteks ini WAN, disebut sebagai jaringan yang tidak aman, karena tidak ada yang tahu, bagaimana perjalanan data melewati WAN. Hal ini mengharuskan Virtual Private

Network untuk memberikan jaminan keamanan pada komunikasi antar dua jaringan yang akan berhubungan.

Dalam melakukan analisa keamanan pada jaringan VPN ini, akan digunakan sebuah aplikasi bernama Wireshark. Aplikasi ini dapat melakukan pengawasan pada setiap paket data yang melewati layer 2 OSI, dalam konteks ini Hub.



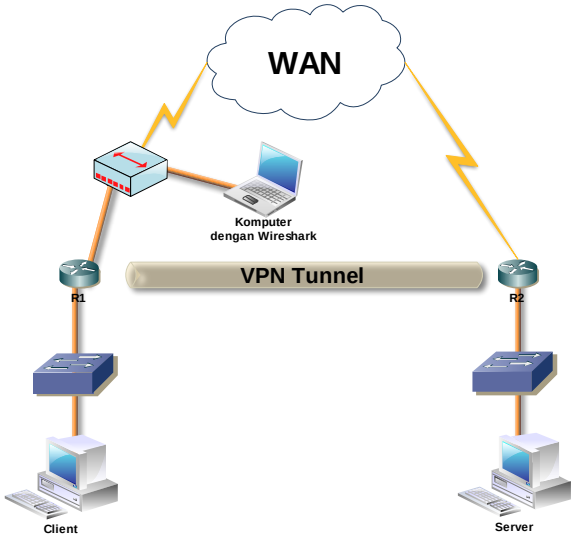
Gambar 1.3
Uji Coba Keamanan Tanpa VPN

Uji coba keamanan akan dilakukan pada beberapa titik yang ada pada jaringan. Pada uji coba pertama akan dilakukan pengiriman data dari satu titik menuju titik yang lain, tanpa menggunakan koneksi VPN pada titik yang berada di antar dua buah gateway VPN. Hasilnya, akan digunakan sebagai variabel kontrol terhadap uji coba berikutnya.

Secara teori, data yang lewat melalui jaringan dapat disadap dan dianalisa melalui Wireshark. Jika tidak mengalami enkripsi, maka isi data dapat dilihat secara langsung, terutama data-data berupa teks. Hal ini tentunya menjadi sebuah ancaman apabila data-data yang dikirimkan merupakan data yang penting, seperti password, informasi kartu kredit, maupun informasi rekening pada bank.

Variabel kontrol, berfungsi sebagai patokan yang membedakan jaringan dengan VPN dan jaringan tanpa VPN. Dengan menggunakan variabel kontrol yang telah diperoleh dari uji coba pertama pada tiga titik

yang berbeda, akan dilakukan uji coba pada jaringan yang menggunakan VPN pada titik yang sama.



Gambar 1.4
Uji Coba Keamanan Dengan VPN

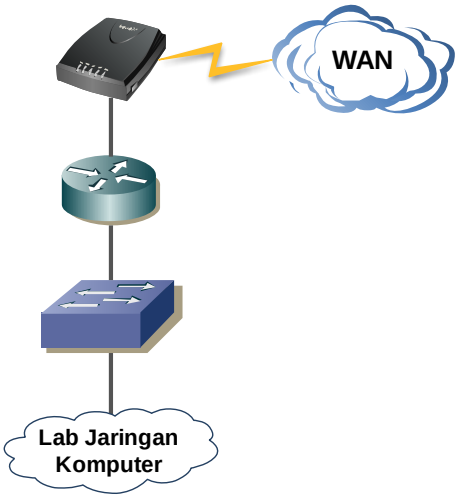
4. Studi Kasus

VPN merupakan sebuah solusi bagi sebuah perusahaan yang membutuhkan komunikasi secara aman antara pusat dan cabang, di mana letak antara pusat dan cabang tersebut saling berjauhan. Ada beberapa metode lain untuk melakukan komunikasi ini, antara lain:

- *Leased Line*
- *Frame Relay*
- ATM
- ATM-to-*Frame Relay Service Internetworking*
- ISDN

Dari beberapa opsi di atas, menawarkan koneksi jaringan secara langsung. Namun biaya yang dibutuhkan cukup besar, sehingga sangat sulit diterapkan oleh perusahaan skala kecil menengah. Oleh karena itu, VPN menjadi sebuah solusi akan jaringan yang aman dan terjangkau.

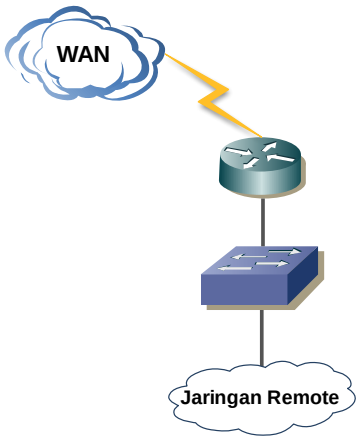
Untuk melakukan analisa terhadap WAN, diperlukan implementasi jaringan yang nyata pada jaringan WAN itu sendiri. Oleh karena itu, pada studi kasus ini, akan diimplementasikan Virtual Private Network menggunakan Router Cisco 1841 antara Laboratorium Jaringan komputer STTS, dengan network lain di luar STTS yang disebut dengan jaringan remote, dengan menggunakan koneksi Internet ADSL. Adapun jaringan yang ada pada Laboratorium Jaringan STTS pada saat ini, dapat digambarkan seperti gambar di bawah ini.



Gambar 1.5
Konfigurasi Jaringan Laboratorium
Jaringan Komputer STTS

Jaringan Laboratorium Jaringan Komputer STTS, terdiri dari sebuah komputer server, sebuah komputer administrator, dan dua puluh buah komputer klien yang terhubung pada sebuah dua buah switch yang terpasang secara seri. Pada gambar di atas, komputer klien hanya diwakili oleh dua buah komputer, dan swith hanya diwakili oleh sebuah switch. Salah satu switch terhubung langsung menuju router server yang menjembatani antara kominikasi antara jaringan Laboratorium Jaringan STTS dengan ADSL Router yang memberikan koneksi Internet, atau WAN.

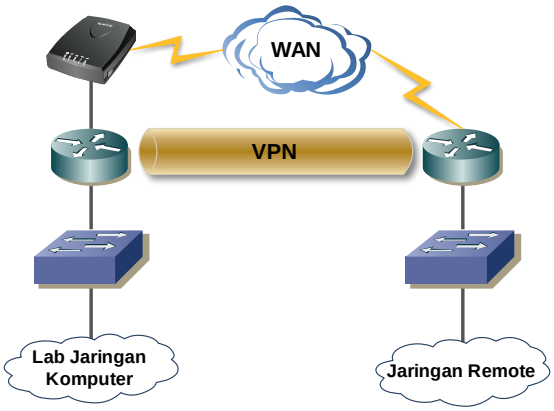
Sedangkan pada network lain yang akan dihubungkan, konfigurasi sederhananya dapat digambarkan pada gambar di bawah ini:.



Gambar 1.6
Konfigurasi Jaringan Remote

Konfigurasi jaringan tidak terlalu berbeda dengan jaringan Laboratorium Jaringan STTS. Dua buah komputer klien dan sebuah laptop terhubung pada sebuah Wireless Router, yang terhubung dengan langsung ADSL Router yang memberikan koneksi Internet, atau WAN.

Konfigurasi kedua jaringan yang telah disebutkan di atas akan ditambahkan Router Cisco 1841 pada masing-masing jaringan sehingga dapat melakukan koneksi Virtual Private Network. Adapun konfigurasi kedua jaringan tersebut akan berubah seperti gambar di bawah ini.



Gambar 1.7
Konfigurasi Jaringan VPN

Pada jaringan Laboratorium Jaringan STTS, koneksi dari switch menuju router server akan dijembatani oleh Router Cisco 1841. Sedangkan pada jaringan remote, Router Cisco 1841 akan diletakkan di antara ADSL Router dan Wireless Router yang menghubungkan komputer klien.

Dengan konfigurasi seperti ini, diharapkan kedua jaringan tersebut memperoleh privasi untuk berhubungan satu sama lain tanpa ada pihak-pihak lain yang tidak berkepentingan yang mampu menyadap komunikasi kedua jaringan tersebut.

5. Target Akhir

   Target akhir yang utama dari tugas akhir ini adalah implementasi VPN IPsec menggunakan koneksi ADSL antar jaringan laboratorium jaringan komputer STTS, dengan jaringan remote di luar STTS menggunakan Router Cisco 1841.

   Selain itu juga uji keamanan dari VPN dengan menggunakan protokol keamanan IPsec, dan protokol kriptografi ISAKMP pada router Cisco 1841. Selain itu uji *performance* juga akan dilakukan berdasarkan kombinasi antara metode-metode yang disediakan oleh protokol IPsec dan ISAKMP.

   Untuk melakukan analisa terhadap performance, akan diperbandingkan metode-metode enkripsi, antara lain DES-CBC, TripleDES-CBC, dan AES-CBC. Unsur yang digunakan untuk proses perbandingan ini adalah waktu dan keamanan paket data, terhadap jumlah router yang digunakan pada WAN, enkripsi dan hash yang digunakan.

1.5. Metodologi

Metodologi yang digunakan untuk menyelesaikan tugas akhir adalah sebagai berikut:

1. Mencari informasi mengenai pengaturan VPN pada WAN.
2. Mencari Sistem Operasi yang mendukung VPN pada Router Cisco 1841.

3. Melakukan peningkatan sistem operasi pada Router Cisco 1841 yang sudah ada sebelumnya menjadi "c1841-advsecurityk9-mz.124-23"melalui tftp server.
4. Mempelajari sistem kerja VPN dan mengimplementasikannya pada Router Cisco 1841.
5. Melakukan konsultasi dengan dosen pembimbing.
6. Melakukan uji coba keamanan pada VPN yang sudah dibuat dengan menggunakan Wireshark.
7. Melakukan implementasi VPN menggunakan koneksi ADSL.
8. Melakukan analisa perbandingan keamanan dari jaringan tanpa VPN dengan jaringan menggunakan VPN.
9. Mencari metode penelitian statistika yang dapat digunakan dalam judul ini.
10. Melakukan analisa perbandingan terhadap performance dari metode-metode yang dimiliki oleh protocol IPsec dan ISAKMP, serta membuat table perbandingannya.

1.6. Sistematika Pembahasan

Buku ini merupakan laporan hasil Studi Analisa tentang Virtual Private Network pada Router Cisco 1841. Pembahasan buku ini adalah mengenai VPN, Router Cisco 1841, dan implementasinya, serta analisa keamanan pada jaringan yang privat yang dihasilkannya. Adapun pembahasan dalam buku ini adalah sebagai berikut:

- BAB I : PENDAHULUAN

  Bab ini menjelaskan latar belakang pembuatan tugas akhir ini beserta tujuannya, ruang lingkup secara singkat, serta sistematika pembahasan apa saja yang akan dibahas nantinya pada buku yang akan dibuat ini

- BAB II : VIRTUAL PRIVATE NETWORK

  Pada bab ini akan dibahas teori dasar dan konsep tentang Virtual Private Network yang nantinya akan diimplementasikan pada bab berikutnya.

- BAB III : IMPLEMENTASI DAN STUDI KASUS

  Bab ini berisi laporan tentang implementasi Virtual Private Network yang sudah dilakukan pada jaringan Laboratorium Jaringan Komputer Sekolah Tinggi Teknik Surabaya dengan Jaringan Remote.

- BAB IV : IPSEC PADA ROUTER CISCO 1841

  Pada bab ini akan dijelaskan uji coba dan analisa yang sudah dilakukan terhadap keamanan Virtual Private Network yang sudah diimplementasikan sebelumnya dengan menggunakan sebuah aplikasi yang bernama WireShark. Serta analisa statistik tentang hubungan antara komponen-komponen yang dianalisa.

- BAB V : PENUTUP

  Pada bab terakhir ini, akan dijabarkan kesimpulan selama melakukan studi analisa hingga saat pembuatan buku laporan tugas akhir ini. Kesimpulan yang diberikan juga akan disertai dengan alasan. Sedangkan saran adalah saran dari penulis mengenai harapan yang harus diperhatikan oleh pembaca saat akan melakukan tugas akhir serupa pada periode-periode selanjutnya.