BAGIAN 1 PENDAHULUAN

1.1.Latar Belakang

Dengan semakin berkembangnya teknologi maka semakin berkembang pula sistem keamanannya. Bagi perusahaan besar mereka membutuhkan penghubung yang dapat menghubungkan kantor cabang mereka dengan kantor pusat, begitu juga sebaliknya, saat data di enkripsi melalui Internet lalu-lintas data mereka melindunginya. Sebagai contoh, sebuah toko retail harus terhubung dengan kantor pusatnya untuk mengetahui persediaan barang dan pemesanan, toko cabang tersebut dapat juga terhubung dengan sesama toko cabang lainnya untuk mengetahui sisa produk yang tersedia. Dahulu, satu-satunya cara untuk menghubungkan cabang dengan pusat ialah dengan menggunakan *Layer-2* seperti ISDN atau *frame relay* untuk saling berkomunikasi. Dengan menggunakan ISDN atau *frame relay* akan memakan banyak waktu dan biaya yang cukup mahal. Jika semua kantor cabang (termasuk kantor pusat) sudah memiliki akses internet yang relatif murah, maka akses internet ini juga dapat digunakan untuk komunikasi IP internal antara cabang dan kantor pusat dengan menggunakan *IPsec tunnels* untuk memastikan privasi dan integritas data.

DMVPN adalah teknologi yang di perkenalkan Cisco untuk mempermudah koneksi antara kantor cabang dengan kantor pusat dan sebaliknya. *DMVPN* merupakan fitur yang ditawarkan oleh Cisco yang dapat memungkinkan pertukaran data melalui internet secara aman, seolah- olah data tersebut dikirimkan melalui perantara kabel. *DMVPN* memiliki banyak fitur dan teknologi seperti *IPSec (IP Security), mGRE (multipoint GRE), NHRP (Next Hope Resolution Protocol)*. Fitur *IPSec* membuat data yang di kirimkan ter-enkripsi dan ter-dekripsi. *IPSec* diibaratkan sebagai *Tunnel* (terowongan) untuk jalur lalu-lintas data.

DMVPN memiliki keunggulan dibandingkan *VPN* biasa, karena *VPN* biasa memiliki konfigurasi yang cukup rumit dan kompleks dalam hal ini pada *VPN* biasa seorang administrator harus memasukkan konfigurasi satu persatu atau *site-to-site*, apabila *site* di tambah maka konfigurasi ditambahkan juga. Berbeda dengan *DMVPN*, apabila ada *site* yang ditambahkan *DMVPN* secara default akan menambahkan *site* tersebut.

Cisco *DMVPN* memungkinkan lokasi cabang untuk berkomunikasi secara langsung satu sama lain melalui WAN publik atau internet, seperti ketika menggunakan *voice over IP (VOIP)* antara dua kantor cabang, tetapi tidak memerlukan koneksi *VPN* permanen antara situs. Hal ini memungkinkan penyebaran zero-touch dari *IPsec VPN* dan meningkatkan kinerja jaringan dengan mengurangi *latency* (jumlah waktu yang dibutuhkan paket data untuk berpindah di seluruh koneksi jaringan) dan jitter (variasi dari delay atau selisih antara *delay* pertama dengan *delay* selanjutnya), sekaligus mengoptimalkan pemanfaatan *bandwidth* kantor pusat.

Sudah selayaknya bagi perusahaan-perusahaan besar untuk membagun koneksi *IPSec* secara besar untuk menghubungkan cabang mereka melalui jaringan internet. *IPSec* mengenkripsi *traffic* antara dua titik (*peer to peer*) dan pengenkripsian tersebut dilalukan kedua titik menggunakan kata kunci yang rahasia. Karena kata kunci rahasia ini hanya terdapat antara kedua titik tersebut, jaringan terenkripsi secara erat antara kedua *peer.* Oleh karena itu, *IPSec* secara interinsik adalah penghubung antara titik *tunnel* dalam jaringan. Metode ini layak di implementasikan untuk jaringan berskala besar dan memiliki titik cabang yang banyak dan untuk mengatur kedalam *hub* dan *spoke* atau secara penuh menggunakan *mesh network.* Dalam sebagian besar jaringan, *traffic* IP antara *spokes* dan *hub* cukup mendominasi dan antar *spoke* sangat kecil, jadi desain *hub* dan *spoke* sering menjadi pilihan utama. Desain ini juga cocok untuk jaringan *Frame Relay* versi lama, maka dari itu biaya yang dikeluarkan juga menjadi cukup mahal.

Ketika menggunakan internet sebagai penghubung antara *hub* dan *spoke*, *spoke* juga memiliki akses langsung ke *spoke* lainnya tanpa adanya biaya tambahan, tetapi cara ini cukup sulit, namun bukan hal yang mustahil untuk mengelola secara penuh maupun sebagian jaringan *mesh* ini. Menghubungkan jaringan secara penuh atau sebagian adalah cara paling menguntungkan karena dapat menghemat biaya jika *spoke* dapat berhubungan langsung dengan *spoke* lainnya tanpa adanya perantara *hub.* Jika lalu lintas antar *spoke* melalui *hub*, maka *hub* akan menggunakan sumberdayanya dan berdampak kepada delay-nya paket data yang dikirim karena hub akan meng-enkripsi *IPSec* dan men-dekripsi paket

data yang datang dari *spoke* pengirim dan di enkripsi kembali sebelum dikirimkan kepada *spoke* penerima. Sebagai contoh lainnya saat *spoke* dan *spoke* terhubung langsung akan sangat berfungsi ketika kedua *spoke* berada di kota yang sama sedangkan *hub* berada di negara atau kota berbeda, maka akan terjadi efisiensi dalam mengelola waktu dan biaya. Judul penelitian "**Konfigurasi *DMVPN* Menggunakan *IPSec* dan *Routing EIGRP* pada PT. Cahaya Kreatif Digital**"

1.2. Perumusan Masalah

Berdasarkan latar belakang diatas, maka permasalah yang akan dikaji pada penelitian ini dapat dirumuskan sebagai berikut:

1. Bagaimana *DMVPN* dapat membuat *transfer* data menjadi efisien?
2. Bagaimana *IPSec* men-*encrypt* data?
3. Apa kelebihan *DMVPN* dibanding *VPN* biasa?

1.3. Tujuan dan Manfaat Penelitian

- Adapun tujuan penulisan tugas akhir ini antara lain:
  - 1.1.1. Menjadikan *DMVPN* dengan *routing EIGRP* sebagai *routing* utama dari perusahaan.
  - 1.1.2. Mengetahui kelebihan dari *IPSec* dibandingkan teknik enkripsi lainnya.
  - 1.1.3. Memahami kelebihan *DMVPN*.
- Manfaat yang diharapkan dari penelitian tugas akhir ini adalah sebagai berikut:
  1. Efisiensi dalam *transfer* data secara *reliable*.
  2. Investasi terhadap *infrastructure*.

1.4. Batasan Masalah

Dalam konfigurasi *DMVPN* menggunakan *IPSec* dan *router EIGRP* ini terdapat beberapa batasan masalah yang ada, yaitu:

1.1.4. Pada laporan ini hanya menampilkan pengiriman data antar *router*.
1.1.5. *Routing* menggunakan *EIGRP*.
1.1.6. *DMVPN* versi ketiga.

1.1.7. Menggunakan *GNS 3* sebagai *software* uji coba.

1.1.8. Menggunakan *Router* Cisco.

1.5. Metode Penelitian

Pada metodologi penelitian ini penulis menjabarkan beberapa hal tentang bagaimana penelitian yang dilaksanakan, antara lain:

1.1.9. Studi Kepustakaan

Dilakukannya pengumpulan referensi mengenai hal-hal yang berhubungan dengan sistem *networking* dengan mengunakan *DMVPN* dan routing EIGRP dan literatur-literatur yang terkait.

1.1.10. Jenis Penelitian

Penelitian ini akan menggunakan metode *Forward Engineering Research*, dilakukan mulai dari identifikasi masalah, pengumpulan data, penyusunan model, pengujian model, pembangunan, evaluasi, dan validasi. Penelitian dilakukan mulai dari abstraksi yang lebih tinggi menuju ke setingkat atau beberapa tingkat lebih rendah, sehingga dapat digunakan untuk menguji teori/ model/ *formula* (*confirmatory research*).

1.1.11. Metode Pengumpulan Data

Data yang akan digunakan dalam penelitian ini merupakan data primer yaitu data yang didapatkan dari PT. Cahaya Kreatif Digital lalu akan di tambah dengan beberapa studi pustaka yang menjadi data sekunder.

1.6. Sistematika Penulisan

Untuk memahami lebih jelas laporan ini, maka materi-materi yang tertera pada laporan skripsi ini dikelompokkan menjadi beberapa sub bab dengan sistematika penyampaian sebagai berikut:

BAB I PENDAHULUAN

Bab yang membahas tentang gambaran penelitian dan dasar masalah yang di lakukan oleh peneliti, yang mencakup latar belakang, identifikasi masalah, batasan masalah, tujuan dan manfaat penelitian serta sistematika penulisan.

BAB II LANDASAN TEORI

Bab yang memaparkan teori – teori yang diperoleh dari sumber-sumber yang relevan untuk digunakan sebagai panduan dalam penelitian serta penyusunan tugas akhir.

BAB III ANALISIS SISTEM

Bab yang menjelaskan tentang gambaran sistem serta deskripsi dari hasil analisis sistem yang akan dijadikan sebagai petunjuk untuk perancangan pada tahapan berikutnya.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab yang menjelaskan mengenai kebutuhan *hardware*, *software* serta mengenai arsitektur dan proses konfigurasi *router* dan melakukan pengujian *ping, next-hop* dan hasil konfigurasi *DMVPN* itu sendiri.

BAB V KESIMPULAN DAN SARAN

Mengemukakan kesimpulan yang diambil dari hasil penelitian dan penulisan tugas akhir ini, serta saran-saran untuk pengembangan selanjutnya, agar dapat dilakukan perbaikan-perbaikan di masa yang akan datang.

DAFTAR PUSTAKA

LAMPIRAN