**STUDI PENGKAJIAN**

**VIRTUAL PRIVATE NETWORK**

**MENGGUNAKAN IPSEC**

**PADA ROUTER CISCO 1841**

Iwan Chandra

Ir. F.X. Ferdinandus, M.T.

***Abstrak*** – Perkembangan teknologi saat ini, telah memaksa semua elemen-elemen kehidupan untuk beradaptasi dengan teknologi tersebut, tidak terkecuali pada sektor bisnis. Dalam perkembangan bisnis tersebut yang tidak menutup kemungkinan akan adanya ekspansi perusahaan. Seiring dengan bermunculannya teknologi Internet dengan biaya yang cukup terjangkau, dibutuhkan sebuah teknologi yang dapat menjamin kerahasiaan dalam komunikasi data yang dilakukan. Sehingga muncul sebuah konsep Virtual Private Network guna memenuhi kebutuhan tersebut.

Dalam implementasinya, terdapat beberapa teknologi Virtual Private Network. Seperti PPTP, L2TP, IPsec, dan beberapa metode lainnya. Dalam implementasi dan uji coba ini, dipilih metode IPsec karena memiliki sebuah framework keamanan yang dapat dimodifikasi sesuai dengan kebutuhan keamanan yang diinginkan. Selain itu, penerapan IPSec juga lebih mudah dibanding protokol yang lainnya, serta mendukung semua modus operasi yang ada. Metode VPN IPsec ini, diaplikasikan pada jalur Internet ADSL menggunakan Router Cisco 1841 dengan menggunakan metode RFC 1843 Bridge pada jaringan Laboratorium Jaringan Komputer STTS, dan modul WIC-1ADSL pada jaringan remote yang terletak di luar STTS. Sehingga akan terbentuk sebuah tunnel IPsec antara kedua jaringan tersebut. Analisa dilakukan pada kombinasi metode-metode enkripsi dan hash yang disediakan oleh Router Cisco 1841, antara lain DES, 3DES, AES, SHA, dan MD5. Selain itu, analisa juga dilakukan dengan menguji keterkaitan antara jumlah router pada WAN dengan kinerja tunnel VPN yang dihasilkan. Dalam analisa ini digunakan metode perhitungan statistik, yaitu Analysis of Variance (ANOVA) dan regresi linear.

Dengan uji coba dan analisa ini, diperoleh beberapa fakta yang dihasilkan berdasarkan perhitungan statistik. Kinerja VPN dipengaruhi oleh metode enkripsi yang digunakan, serta jumlah router yang terlibat pada WAN. Selain itu, VPN mengurangi kinerja jaringan sebesar 44.44% dari jaringan normal. Dengan biaya yang cukup rendah, VPN lebih layak untuk diaplikasikan pada perusahaan kecil dan menengah.

***Kata Kunci –*** Virtual Private Network, IPsec, ADSL, Cisco 1841.

**I. Pendahuluan**

Pada perkembangan jaringan hingga saat ini, sudah muncul beberapa perangkat yang berguna untuk menghubungkan jaringan. 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 table 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.

**II. Virtual Private Network**

Internet merupakan sebuah solusi komunikasi. Namun keamanan Internet sedikit dipertanyakan, karena tidak ada yang tahu secara pasti apa yang terjadi pada data saat dikirimkan melalui Internet. Sehingga sangat mungkin sekali, bahwa data yang dikirimkan, dapat disadap oleh pihak-pihak yang tidak bertanggung jawab.

Sehingga untuk memenuhi kebutuhan komunikasi yang aman, terdapat beberapa pilihan solusi antara lain:

* Leased Line
* Dial Up
* Frame Relay
* Asynchronous Transfer Mode (ATM)

Internet merupakan sebuah solusi komunikasi dengan biaya yang dapat dikatakan cukup terjangkau. Oleh karena itu, untuk membentuk sebuah komunikasi yang aman dan terjangkau, timbullah sebuah konsep yang bernama Virtual Private Network.

Virtual Private Network adalah fasilitas yang memungkinkan koneksi jarak jauh (remote access) yang aman dengan memanfaatkan jaringan Internet untuk melakukan akses menuju jaringan yang dituju.

Virtual Private Network memberikan beberapa keuntungan, yaitu:

* Hemat Biaya
* Keamanan .
* Skalabilitas
* Kompatibel dengan teknologi broadband yang ada

Berdasarkan cara koneksinya, Virtual Private Network dapat dibagi menjadi dua tipe:

* Site to Site VPN
* Remote User VPN

IPsec merupakan sebuah standar IETF (RFC 2401-2412) yang mendefinisikan bagaimana VPN dapat diatur menggunakan protokol pengalamatan IP atau IP addressing protocol.

IPsec tidak terikat dengan metode enkripsi, autentikasi, algoritma keamanan, maupun teknologi penguncian tertentu. IPsec merupakan sebuah framework terbuka standar yang memperinci aturan-aturan yang dibutuhkan untuk keamanan komunikasinya. IPsec bergantung pada algoritma yang telah ada sebelumnya untuk mengimplementasikan enkripsi, autentikasi, dan pertukaran kunci atau key exchange.



**Gambar 1. Topologi IPsec VPN**

IPsec mampu mengamankan jalur di antara sepasang gateway, sepasang host, maupun gateway dan host. Dengan menggunakan IPsec framework, IPsec menyediakan beberapa fungsi keamanan esensial:

* Kerahasiaan (Confidentiality)
* Integritas / Keaslian (Integrity)
* Autentikasi (Authentication)
* Security Key Exchange

**III. Implementasi dan Studi Kasus**

Untuk membentuk sebuah jaringan VPN dalam pembahasan studi kasus ini, dibutuhkan beberapa komponen pendukung. Berikut ini komponen-komponen yang diperlukan untuk mendukung implementasi studi kasus ini:

* Router Cisco 1841 dengan Sistem Operasi “c1841-advsecurityk9-mz.124-23.bin”
* Koneksi Internet ADSL dengan IP publik statis

Dalam tugas akhir ini, akan diimplementasikan sebuah jaringan VPN yang menghubungkan Laboratorium Jaringan Komputer dengan Jaringan Remote. Di mana kedua jaringan tersebut memilik privasi, dalam komunikasinya melalui jaringan publik. Adapun konfigurasi jaringannya tergambar pada gambar berikut ini.

****

**Gambar 2. Jaringan VPN yang Akan Dibuat**

Terdapat tiga buah metode yang dapat digunakan dalam studi kasus ini, antara lain:

* RFC 1483 Bridged
* Port Forwarding
* Penambahan modul ADSL pada Router Cisco 1841

Ilustrasi jaringan Laboratorium Jaringan Komputer dapat dilihat pada gambar berikut ini.



**Gambar 3. Jaringan Laboratorium Jaringan Komputer**

Setelah router ADSL diatur ke dalam mode bridge, maka Router Cisco 1841 harus dikonfigurasi pada kedua interface Fast Ethernet yang dimiliki. Interface Fast Ethernet 0/0 digunakan untuk jaringan lokal, sedangkan interface Fast Ethernet 0/1 diatur agar dapat melakukan dial up. Proses dial up merupakan proses request menuju ISP. Adapun konfigurasi selengkapnya adalah sebagai berikut.

1. Konfigurasi alamat IP Fast Ethernet 0/0
2. Pembuatan Virtual Private Dialer Network
3. Konfigurasi Interface Fast Ethernet 0/1 sebagai interface WAN
4. Konfigurasi Interface Dialer
5. Konfigurasi Credential dari ISP
6. Konfigurasi Routing Protocol
7. Konfigurasi Access List
8. Konfigurasi Network Address Translation (NAT)
9. Pembentukan IKE Policies
10. Konfigurasi Pre-shared Key
11. Konfigurasi IPSec Transform Set
12. Pendefinisian jalur khusus pada ACL
13. Pembuatan dan Aplikasi Crypto Map

Ilustrasi Jaringan Remote dapat dilihat pada gambar di bawah ini.



**Gambar 4. Jaringan Remote**

Berikut ini tahap-tahap konfigurasi yang dilakukan pada Router 2 yang berada pada Jaringan Remote.

1. Konfigurasi alamat IP Fast Ethernet 0/0
2. Konfigurasi Interface ADSL
3. Konfigurasi Dialer
4. Konfigurasi Default Route Dialer 1
5. Konfigurasi Network Address Translation
6. Pembentukan IKE Policies dan Pre-shared Key
7. Konfigurasi IPSec Transform Set
8. Pendefinisian jalur khusus pada Access List
9. Pembuatan dan Aplikasi Crypto Map

Dengan demikian konfigurasi dari Router 2 yang terletak pada Jaringan Remote telah selesai. Sehingga uji coba koneksi antara kedua router yang bertindak sebagai gateway VPN dapat dilakukan. Uji coba dilakukan dengan melakukan PING dari router.

**IV. IPsec pada Router Cisco 1841**

Dalam uji coba dan analisa ini, akan diperbandingkan beberapa kombinasi dari metode enkripsi dan hash yang disediakan oleh framework IPSec yang dimiliki oleh Router Cisco 1841 dengan sistem operasi “c1841-advsecurityk9-mz.124-23.bin”. Berikut ini metode-metode enkripsi dan hash yang akan digunakan oleh dalam studi analisa ini:

**Tabel 1**

**Metode-Metode IPsec Yang Akan Digunakan**

|  |  |
| --- | --- |
| **Enkripsi** | DES |
| 3DES |
| AES |
| **Hash** | SHA |
| MD5 |

Pada uji coba dan analisa ini, hanya digunakan autentikasi dengan metode pre-shared key saja, karena implementasi RSA, baik RSA Encryption maupun RSA Signature, membutuhkan sebuah digital certificate yang diterbitkan oleh perusahaan keamanan seperti Cybertrust dan Verizone.

Dalam uji coba ini, digunakan tiga buah skenario WAN untuk menguji performa dari koneksi VPN yang dibentuk oleh kedua gateway VPN. Adapun tiga buah skenario tersebut yaitu:

* 0 Router
* 2 Router
* 6 Router

Jaringan komunikasi yang terbentuk antara kedua sub-jaringan tersebut, masih merupakan jaringan publik yang dikatakan tidak aman. Karena paket yang dikirimkan, tidak mengalami enkripsi sama sekali sejak keluar dari komputer. Oleh karena itu, perlu dibentuk sebuah jaringan VPN yang dapat diibaratkan sebagai sebuah tunnel atau terowongan.



**Gambar 5. VPN Tunnel**

Berdasarkan analisa yang telah dilakukan pada bab ini, dapat diambil kesimpulan:

* VPN IPsec menurunkan kinerja suatu jaringan 44.44%.
* Jumlah router pada WAN berpengaruh pada performa VPN.
* Metode hash tidak berpengaruh pada performa VPN.
* Metode enkripsi berpengaruh pada performa VPN.
* Interaksi antara metode hash dengan jumlah router pada WAN tidak berpengaruh pada performa VPN.
* Interaksi antara metode enkripsi dengan jumlah router pada WAN berpengaruh pada performa VPN.
* Interaksi antara metode hash dengan metode enkripsi tidak berpengaruh pada performa VPN.
* Interaksi antara metode hash, metode enkripsi, dan jumlah router pada WAN tidak berpengaruh pada performa VPN.
* VPN tergolong lebih murah dibandingkan dengan Leased Line, sehingga lebih cocok untuk diaplikasikan pada perusahaan kecil menengah.

Terdapat sebuah aplikasi dengan nama Cisco Configuration Proffesional, yang dapat mempermudah konfigurasi dari Router Cisco 1841, mulai dari pengaturan interface, maupun pembentukan security policy, dan firewall. Namun penggunaan aplikasi ini, belum sepenuhnya terlepas dari penggunaan CLI pada Router Cisco 1841.

**V. Penutup**

Berikut ini kesimpulan-kesimpulan dari dari implementasi dan studi analisa yang sudah dilakukan pada tugas akhir ini:

* VPN IPsec dapat diaplikasikan menggunakan Router Cisco 1841 pada jalur ADSL dengan metode bridging pada modem ADSL, maupun penambahan modul WIC-1ADSL pada router Cisco 1841.
* Performa atau kinerja VPN dipengaruhi oleh metode enkripsi, jumlah router pada WAN, serta interaksi dari keduanya. Sehingga metode hash yang digunakan tidak memberikan pengaruh apapun bagi kinerja VPN. Jumlah router yang dilalui pada WAN mempengaruhi performa dan kinerja VPN IPsec.
* Kinerja VPN IPsec menurun sebesar 44.44% dibandingkan dengan jaringan normal, hal ini disebabkan oleh enkripsi dan dekripsi yang membutuhkan waktu dalam prosesnya.
* Dengan biaya yang cukup rendah, VPN lebih pantas untuk diaplikasikan pada perusahaan kecil dan menengah.
* Cisco Configuration Proffesional mempermudah dalam proses konfigurasi Router Cisco 1841. Meskipun demikian, penggunaannya tidak dapat terlepas dari Command Line Interface dan Console Port.

**Referensi**

1. Anonim, Analisis Varians, <http://id.wikipedia.org/wiki/Analisis_varians>, Agustus 2012.
2. Anonim, Regresi Linear, <http://www.konsultanstatistik.com/2009/03/regresi-linear.html>, Agustus 2012.
3. Anonim, Telkom Product and Services, <http://www.telkom.co.id/products-services/>, September 2012.
4. Anonim, SolusiNet Indonesia Pricing, <http://www.solusi.net.id/services.php?p=Leased%20Line>, September 2012.
5. Cisco, 2010, Cisco Router Guide for Teleworkers, Small Offices, Small to Medium-sized Businesses, and Enterprise Branch and Head Offices V.6, San Francisco: Cisco
6. Hicks, Charles R. 1993, Fundamental Concepts in the design of Experiments, New York: Oxford University.
7. Junaidi, Titik Presentasi Distribusi F Probabilita = 0.05, <http://junaidichaniago.wordpress.com>, 2010.
8. Rafiudin, Rahmat, 2003, Mengupas Tuntas Cisco Router. Jakarta: Elex Media Komputindo.
9. Sadikin, Nanang, 2009, Mastering VPN Client Access di Windows Server 2008, Yogyakarta: Penerbit Andi.
10. Santoso, Singgih, 2003, Mengatasi Berbagai Masalah Statistik dengan SPSS Versi 11.5, Jakarta: Elex Media Komputindo.
11. Sudjana, Prof, DR, M.A., M. Sc., 1995, Desain dan Analisis Eksperimen, Bandung: Tarsito.
12. Sunyoto, Aris Wendy, 2006, VPN, Sebuah Konsep, Teori, dan Implementasi, Surabaya: Bukuweb.com.