Seminar Nasional Aplikasi Teknologi Informasi 2005 (SNATI 2005) *ISBN: 979-756-061-6*
Yogyakarta, 18 Juni 2005

IPSEC SEBAGAI SALAH SATU SOLUSI KEAMANAN DATA PADA JARINGAN KOMPUTER

Agustinus Noertjahyana, Rudy Adipranata
Universitas Kristen Petra, Jl. Siwalankerto 121-131, Surabaya
E-mail: agust@petra.ac.id, rudya@petra.ac.id

Abstrak

Pada sebuah jaringan komputer, keamanan data sangatlah penting, terutama jika data tersebut bersifat rahasia. Namun saat ini masih banyak pengguna komputer terutama masyarakat awam yang kurang mengerti betapa penting arti dari keamanan sistem. Di samping itu juga dikarenakan untuk melakukan proses pengamanan terhadap suatu sistem terasa begitu sulit dan membutuhkan tahapan yang agak rumit. Biasanya setelah merasakan dampak yang terjadi pada saat sesudah terjadi penyerangan pada sistem, baru berpikir untuk melakukan tindakan pencegahan. Hal ini tentu sangat tidak menguntungkan. Alangkah baiknya apabila dapat melakukan pencegahan sebelum terjadi serangan.

Saat ini terdapat beberapa alternatif metode untuk keamanan data pada jaringan, misalnya dengan mengenkripsi data sebelum dikirimkan, menggunakan tandatangan digital (digital signature), memasang firewall sehingga tidak ada penyusup dari luar yang dapat masuk ke jaringan komputer internal dan lain-lain. Beberapa solusi diatas dapat digunakan untuk meningkatkan keamanan, namun juga terdapat kelemahan, seperti penggunaan firewall dapat mencegah penyusup dari luar, tetapi tidak dapat mencegah jika data disadap oleh orang yang berada dalam jaringan itu sendiri. Begitu pula dengan enkripsi data ataupun tandatangan digital, hal ini membutuhkan kesadaran dari pihak pengirim data untuk melakukan enkripsi yang terkadang terasa merepotkan dan seringkali tidak dilakukan.

Salah satu solusi untuk meningkatkan keamanan data pada jaringan komputer dengan protokol TCP/IP adalah dengan menggunakan IPSec. IPSec ini bekerja dengan melakukan enkripsi pada data sebelum dikirimkan secara otomatis tanpa campur tangan pihak pengirim. Dengan menggunakan IPSec, maka seandainya data berhasil disadap oleh pihak ketiga, data tersebut telah terenkripsi sehingga sangat sulit untuk dapat mengetahui data aslinya. Dan yang lebih penting lagi adalah kemudahan dalam implementasi pada suatu sistem, sehingga dapat menjadikan para pengguna komputer untuk berpikir kembali akan pentingnya keamanan data pada suatu sistem.

Kata kunci: *keamanan jaringan komputer TCP/IP, IPSec.*

1. PENDAHULUAN

Dalam sebuah jaringan komputer, keamanan di dalam pengiriman serta penerimaan data sangat penting untuk menjamin bahwa data yang dikirim tidak jatuh ke pihak ketiga, terutama jika data tersebut bersifat rahasia. Untuk itu perlu dilakukan implementasi metode-metode pengamanan data pada jaringan. Banyak metode yang dapat diimplementasikan, seperti penggunaan tanda tangan digital, enkripsi ataupun pemasangan *firewall* (Tanenbaum, 2003).

Pada jaringan yang berhubungan dengan internet, maka pemasangan *firewall* menjadi wajib karena dengan adanya *firewall*, maka pihak dari luar tidak dapat memasuki jaringan internal kecuali diijinkan. *Firewall* ini efektif untuk mencegah pencurian data ataupun masuknya penyusup yang hendak mengacaukan sistem jaringan. Tetapi dengan adanya *firewall*, tetap tidak bisa mencegah penyadapan data yang dilakukan oleh pihak di dalam jaringan itu sendiri. Cara lain untuk meningkatkan keamanan data adalah dengan menggunakan enkripsi pada data yang akan dikirimkan. Jika data yang dikirimkan berupa file, maka dilakukan enkripsi pada file tersebut sehingga data file tersebut tidak bisa dibaca lagi dengan menggunakan cara biasa, tetapi harus dilakukan pengembalian enkripsi (*decode*) sehingga data file tersebut kembali normal. Untuk melakukan hal ini, maka pihak pengirim harus proaktif dengan melakukan prosedur enkripsi sebelum dia mengirimkan file tersebut. Begitu pula dengan pihak penerima harus melakukan *decode* sehingga file yang diterima dapat diakses secara normal. Seringkali hal tersebut dianggap merepotkan sehingga pihak pengirim tidak melakukan enkripsi terhadap file yang akan dikirimnya sehingga jika file tersebut ditangkap oleh pihak ketiga maka dapat diakses dengan mudah oleh pihak yang tidak dikehendaki tersebut. Untuk pengiriman surat elektronik (*email*), dapat diamankan dengan menggunakan tanda tangan digital (*digital signature*). Tetapi hal ini juga memerlukan kesadaran dari pihak pengirim email untuk mengimplementasikan tanda tangan digital pada email yang dia kirim, dimana hal ini seringkali juga diabaikan.

Salah satu cara untuk mengatasi masalah-masalah yang timbul dari implementasi metode keamanan di atas yaitu dengan menggunakan IPSec. IPSec ini adalah suatu cara untuk

ISBN: 979-756-061-6

meningkatkan keamanan pengiriman data khususnya pada jaringan komputer yang menggunakan protokol TCP/IP (Huggins, 2004). IPSec bekerja dengan melakukan enkripsi pada data yang dikirim secara otomatis tanpa campur tangan pihak pengirim (Jones, 2003). Seandainya data yang telah dienkripsi oleh IPSec ini dapat disadap oleh pihak ketiga, data tersebut tidak dapat terbaca jika tidak mengetahui kunci enkripsi yang digunakan. Dengan menggunakan IPSec ini terdapat tiga keuntungan yaitu pertama adalah keamanan data itu sendiri, kedua adalah otentikasi dimana IPSec akan menandai data yang dikirim dengan kunci enkripsi sehingga pihak penerima dapat yakin bahwa data yang dikirim berasal dari pihak pengirim yang benar, bukan berasal dari pihak lain yang menyamar sebagai pihak pengirim. Dan keuntungan terakhir adalah integritas data karena IPSec melakukan perhitungan checksum yang akan dicocokkan saat data tiba di pihak penerima. Dengan checksum ini, pihak penerima dapat yakin bahwa data tersebut tidak dilakukan modifikasi di tengah perjalanannya oleh pihak lain.

2. IPSEC

IPSec dapat menjaga keamanan data pada lalu lintas jaringan dengan menerapkan kebijakan-kebijakan keamanan (Chorafas). Adapun kebijakan-kebijakan keamanan dengan menggunakan IPSec itu terdiri dari satu aturan atau lebih yang menentukan response dari sebuah komputer terhadap lalu lintas IP. Untuk dapat mengimplementasikan IPSec, maka hal yang perlu dilakukan pertama kali adalah dengan membuat suatu kebijakan yang terkait dengan masalah keamanan. Ada kemungkinan terdapat beberapa kebijakan keamanan yang dibuat dengan menggunakan IPSec, namun pada suatu saat hanya bisa menerapkan satu kebijakan pada suatu komputer.

Setiap aturan yang ada dalam suatu kebijakan kemanan terdiri suatu *filter list*, suatu *filter action* dan suatu metode autentikasi.

- Suatu *filter list* dapat mengidentifikasi tipe dari lalu lintas jaringan dan mengacu kepada kebijakan keamanan yang sudah dibuat manakala ada yang cocok dengan kondisi-kondisi yang ada pada *filter list*. Sebagai contoh, suatu *filter list* mungkin saja hanya mengidentifikasi lalu lintas *Internet Control Message Protocol* (ICMP) dan *Hypertext Transfer Protocol* (HTTP).
- Suatu *filter action* menyatakan tindakan-tindakan yang harus dilakukan jika lalu lintas pada jaringan sesuai dengan kondisi-kondisi yang ada pada *filter list*. Suatu *filter action* didefinisikan oleh seorang administrator dengan tujuan mengijinkan, menolak, atau untuk autentikasi terhadap lalu lintas data yang masuk maupun keluar pada saat suatu kondisi terpenuhi. Sebagai contoh, seorang administrator dapat menyaring semua lalu lintas ICMP dan melakukan enkripsi terhadap lalu lintas HTTP. *Filter action* dapat juga menentukan algoritma hash dan enkripsi yang akan digunakan pada kebijakan keamanan tersebut.
- Kebijakan keamanan yang lainnya adalah mengijinkan lalu lintas IP tertentu untuk dapat lewat pada jaringan dengan syarat pengirim dapat melakukan proses autentikasi terhadap identitasnya. Terdapat tiga metode untuk autentikasi yaitu *certificates*, protokol *Kerberos*, sebuah *preshared key*. Suatu aturan yang dibuat dapat menggunakan salah satu metode atau lebih tergantung dari kebutuhan akan keamanan data.

Beberapa aturan yang sudah didefinisikan secara default antara lain: *Default Response*, *Permit ICMP* serta *Encapsulating Security Payload* (ESP).

- *Default Response* meyakinkan bahwa respon dari suatu komputer akan masuk ke jalur komunikasi yang aman. Jika pada kebijakan keamanan dengan menggunakan IPSec pada suatu komputer tidak mempunyai aturan yang sudah didefinisikan untuk komputer lain yang meminta jalur komunikasi yang aman, maka aturan pada *Default Response* akan diaplikasikan untuk melakukan negosiasi dengan penggabungan keamanan.
- *Permit ICMP* mengijinkan lalu lintas ICMP untuk dapat melewati suatu jaringan. ICMP itu sendiri adalah suatu protokol pada lingkungan TCP/IP, yang berguna untuk menyatakan error dan mampu untuk menyederhanakan koneksi yang terjadi. Fitur-fitur yang seperti *File Sharing*, perintah ping dan tracert, serta aplikasi-aplikasi yang lain membutuhkan lalu lintas ICMP supaya dapat melewati suatu jaringan.
- ESP dapat digunakan dalam suatu kebijakan keamanan ketika data akan dikirim melalui Internet. ESP menyediakan service berupa pengiriman data secara aman dengan cara melakukan enkripsi pada lalu lintas jaringan. Selain itu ESP juga menyediakan jasa layanan autentikasi data serta pengecekan terhadap integritas dari suatu data.

Ada beberapa kebijakan keamanan secara default pada Windows 2003 (Huggins), antara lain: Client (Respond Only), Server (Request Security), serta Secure Server (Require Security).

- Client (Respond Only) digunakan pada saat komputer meminta komputer lain untuk menggunakan IPSec. Suatu komputer tidak menggunakan IPSec untuk merespon sampai komputer lain menyatakan permintaan secara

ISBN: 979-756-061-6

khusus. Client (Respond Only) hanya menggunakan aturan Default Response.

- Server (Request Security) digunakan pada server maupun client. Pada saat policy ini diimplementasikan pada suatu komputer, maka komputer akan berkomunikasi dengan server menggunakan IPSec. Namun, komputer server akan berkomunikasi dengan menggunakan jalur biasa jika suatu client tidak di konfigurasi dengan menggunakan IPSec. Pada jalur komunikasi yang tidak aman, IPSec tidak digunakan. Server (Request Security) policy menggunakan aturan Default Response rule, Permit ICMP rule, serta ESP rule.
- Secure Server (Require Security) digunakan pada server dan client secara bersama-sama. Policy ini menggunakan IPSec untuk melakukan komunikasi dan tidak akan pernah berpaling pada jalur komunikasi yang tidak aman. Secure Server policy terdiri dari Default Response rule, Permit ICMP rule, serta ESP rule. Jika Secure Sever (Require Security) ini digunakan, maka semua lalu lintas harus di enkripsi dengan menggunakan ESP pada server supaya dapat berkomunikasi dalam suatu jaringan.

3. IMPLEMENTASI IPSEC

Untuk dapat mengimplementasikan IPSec, hal yang penting adalah dengan memastikan bahwa ada hubungan yang cocok di antara komputer-komputer yang akan melakukan komunikasi. Level keamanan yang ada pada data dalam jaringan akan sangat bergantung pada level keamanan yang sudah di spesifikasikan pada IPSec dari semua komputer yang melakukan negosiasi. Jika pada kedua komputer mempunyai kebijakan keamanan yang saling melengkapi, maka dapat melakukan komunikasi dengan menggunakan IPSec. Namun sebaliknya jika terjadi konflik pada kebijakan keamanan dari masing-masing komputer, maka komunikasi akan dilakukan dengan melalui jalur yang tidak aman, atau bahkan tidak akan melakukan komunikasi sama sekali.

Adapun untuk mengetahui lebih jelas hubungan komunikasi yang terjadi dengan menggunakan kebijakan secara default, dapat dilihat pada tabel 1.

Tabel 1. Komunikasi yang terjadi antar komputer pada Default Policy

	No policy assigned	***Client (Respond Only)***	***Server (Requests Security)***	***Secure Server (Require Security)***
No policy assigned	No IPSec	No IPSec	No IPSec	No communication
Client (Respond Only)	No IPSec	No IPSec	IPSec	IPSec
Server (Requests Security)	No IPSec	IPSec	IPSec	IPSec
Secure Server (Require Security)	No communication	IPSec	IPSec	IPSec

Ketika akan mengimplementasikan IPSec, hal yang penting untuk diketahui adalah adanya suatu keseimbangan antara mengamankan data dari user yang tidak berhak dan membuat user yang punya akses untuk dapat masuk ke dalam jaringan. Untuk itulah, hal yang perlu dilakukan adalah dengan melakukan analisis resiko pada jaringan, menentukan level keamanan yang diperlukan pada suatu organisasi, serta melakukan identifikasi terhadap informasi-informasi yang perlu untuk dilindungi dari serangan pada jaringan. Sangat penting untuk menentukan cara terbaik implementasi kebijakan keamanan pada suatu organisasi yang sudah ada dan memastikan tidak terjadi masalah baik dari sisi manajerial maupun teknis. Hal terbaik adalah dengan memberikan user hak akses terhadap sumber daya hanya sebatas pada kepentingannya serta memastikan bahwa user melakukan akses terhadap suatu sumber daya secara aman dan efisien.

Untuk implementasi kebijakan keamanan dengan menggunakan IPSec, terdapat tiga tingkatan level keamanan (Jones), yaitu:

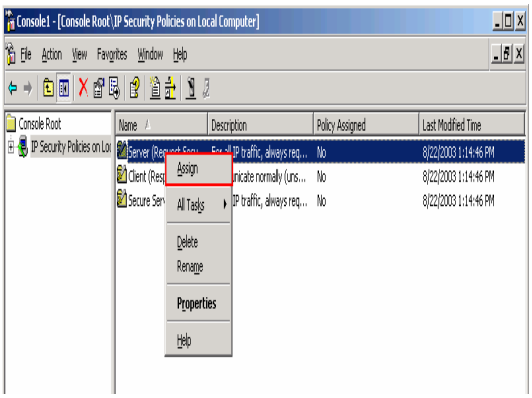
a. Level keamanan minimal. Level keamanan ini dapat digunakan pada komputer yang tidak melakukan komunikasi dengan data yang penting melalui jaringan. IPSec secara default tidak aktif pada level keamanan ini.
b. Level keamanan tingkat standard. Level keamanan ini dapat digunakan ketika hendak menyimpan data penting pada komputer. Level keamanan ini akan menjaga keseimbangan antara kerja efisien dengan keamanan. Client (Respond Only) dan Server (Request Security) memberikan level keamanan Standard.
c. Level keamanan tingkat tinggi. Level keamanan ini digunakan ketika komputer menyimpan data yang sangat penting dan sangat beresiko terhadap akses yang tidak diinginkan. Pada level keamanan ini, jalur komunikasi yang tidak aman antar komputer yang tidak mempunyai IPSec tidak akan diijinkan. Kebijakan Secure Server (Require

ISBN: 979-756-061-6

Security) memberikan level keamanan tingkat tinggi.

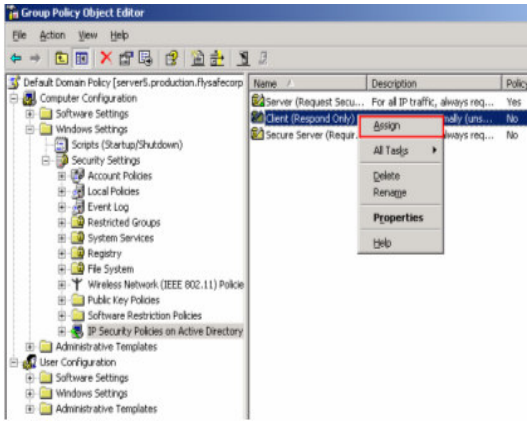
Adapun langkah-langkah untuk implementasi IPSec pada Microsoft Windows Server 2003 adalah sebagai berikut:

- Untuk implementasi IPSec pada Server, maka langkah yang dapat dilakukan adalah dengan cara masuk de dalam IP *Security Policies* setelah itu *assign* kebijakan Server ataupun Secure Server. Untuk lebih jelasnya dapat dilihat pada gambar 1.



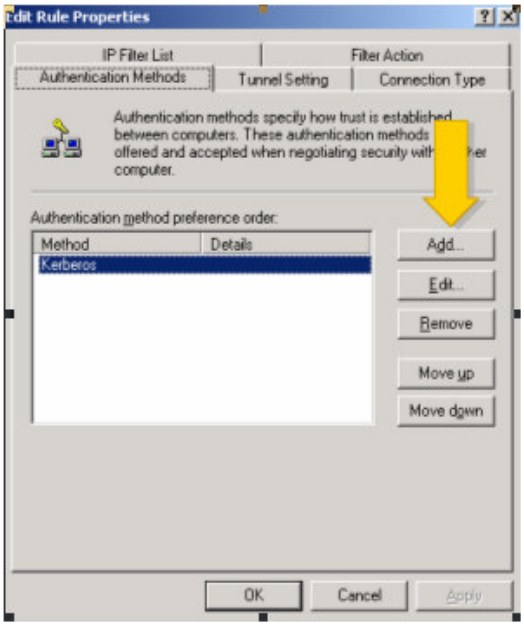
Gambar 1. Pemilihan Jenis Kebijakan IPSec

- Untuk Client dapat dilakukan dengan cara yang sama seperti pada Server, namun yang membedakan adalah dengan *assign* pada kebijakan Client.
- Sedangkan pada Active Directory, maka langkah-langkah yang dilakukan adalah dengan cara melakukan edit pada *Group Policy Editor*. Untuk lebih jelasnya dapat dilihat pada gambar 2.



Gambar 2. Group Policy Editor

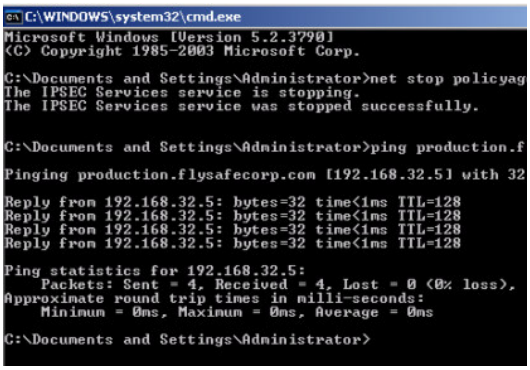
- Untuk mengaktifkan proses autentikasi di antara 2 komputer yang menggunakan IPSec, maka dapat dilakukan dengan cara menambah jenis autentikasi yang ada, dimana secara default adalah dengan menggunakan *Kerberos*. Dengan menggunakan *Kerberos*, maka tidak diperlukan lagi konfigurasi yang lain. Sehingga dapat membantu seorang administrator dalam pekerjaannya. Untuk lebih jelasnya dapat dilihat pada gambar 3.



Gambar 3. Edit Rule Properties

4. HASIL PENELITIAN DAN PEMBAHASAN

Setelah semua tahapan dalam implementasi IPSec sudah dilakukan, maka perlu dilakukan pengamatan untuk memastikan bahwa IPSec dapat berjalan dengan baik. Cara termudah yang dapat dilakukan adalah dengan menggunakan *command ping* untuk melakukan verifikasi terhadap komunikasi. Gambar 4 menunjukkan jaringan yang valid.

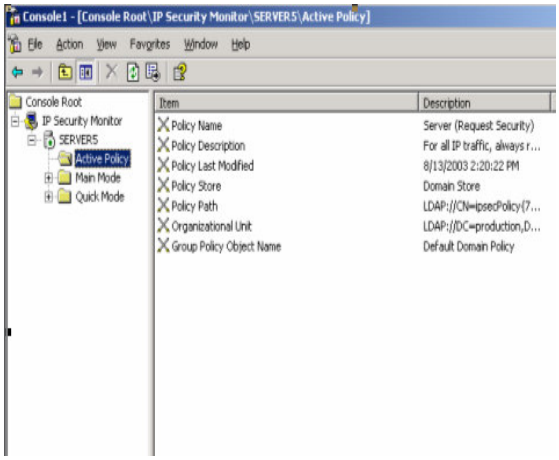


Gambar 4. Koneksi yang terjadi pada jaringan yang valid.

Apabila percobaan koneksi jaringan dengan menggunakan perintah *ping* tidak berhasil, maka dapat dilakukan dengan cara menghentikan IPSec

ISBN: 979-756-061-6

untuk kemudian dijalankan kembali. Hal ini harus dilakukan pada semua komputer yang akan melakukan komunikasi.
Namun terkadang, ada juga permasalahan bahwa dua komputer yang sebetulnya tidak berhak melakukan komunikasi namun tetap saja bisa melakukan komunikasi. Hal ini biasanya dapat dilihat dan diamati dengan menggunakan IPSec Monitor, yang dapat dilihat pada gambar 5.



Gambar 5. IPSec Monitor

5. KESIMPULAN

Dengan menggunakan IPSec, maka keamanan pada jaringan komputer akan meningkat karena IPSec melakukan enkripsi terhadap data yang dikirim pada jaringan tersebut. Seandainya terjadi penyadapan data oleh pihak ketiga, maka data asli tidak dapat dilihat dengan mudah tanpa mengetahui kunci enkripsi yang digunakan.

IPSec akan melindungi data secara otomatis tanpa sepengetahuan pengguna jaringan komputer sehingga pengguna dapat melakukan pengiriman data seperti biasa tanpa ada prosedur khusus yang harus dilakukan.

Implementasi IPSec dapat dilakukan dengan mudah sehingga tidak memerlukan keahlian khusus yang harus dimiliki administrator jaringan.

Daftar Pustaka

[1] Chorafas, D.M., 1984, *Designing and Implementing Local Area Network*, MacGraw-Hill, New York.
[2] Huggins, D., 2004, *Windows Server 2003 Network Infrastructure*, QUE, Indianapolis.
[3] Jones, D., 2003, *Microsoft Windows Server 2003*, QUE, Indianapolis.
[4] Tanenbaum, A.S., 2003, *Computer Networks*, Prentice Hall, New Jersey.