ANALISIS DAN OPTIMALISASI KEAMANAN JARINGAN MENGGUNAKAN PROTOKOL IPSEC

Syarif Hidayatulloh
Universitas BSI
Jalan Sekolah Internasional No.1-6 Antapani, Bandung 40282
syarif.sfq@bsi.ac.id

Abstract *- Data network secure is very important, especially if the data is secret. However, the refuge of the data is usually considered as unimportant thing and less monitored by the user. Because, the data security system is difficult to be applied by the user either in personal computer or in the company. It becomes more important to be applied when the data have been attacked or stolen. It is better for the user to anticipate before it's too late. There are so many ways to protect data in a network computer. For instance, encryption, digital signature, firewall and so on. Some solutions can be applied to increase security system based on the needs of network. It is caused by other factors in the priority system secure such as performance, network specification, device specification, and the cost. IPsec is one of solution to increase the data computer network secure which is supporting many authentic and encryption methods. IPsec work by processing encryption the data before it has been sent automatically. Thus, although the data was successfully intercepted by a third, then the data would not be useful because the data has been encrypted. IPSec also check the data integrity and authenticity fromthe source. In addition, the more important is the ease of implementation does not require high system requirements and certainly low cost. So, the user can realize to apply the secure system immediately.*

Keywords*: Network security, Data security, IPSec*

Abstrak - Keamanan lalu lintas data pada jaringan komputer sangatlah penting, terutama jika data bersifat rahasia. Namun keamanan data masih menjadi sesuatu hal yang dirasa kurang panting dan tidak mendapat perhatian dari pengguna komputer. Ini dikarenakan pengamanan data masih dirasakan sulit untuk diterapkan oleh penguna komputer baik pribadi ataupun diperusahaan. Pengamanan data mulai dianggap penting untuk diterapkan ketika telah terjadi penyerangan atau pencurian data. Ini tentunya Sudah terlambat Karena seharusnya kita sebagai pengguna berfikir cara pencegahan bukan mencegah setelah terjadi. Karena hal tersebut akan sangat merugikan. Banyak cara dalam pengamanan data pada sebuah jaringan komputer, misalnya enkripsi, digital *signature*, *firewall* dan masih banyak lagi. Beberapa solusi dapat diterapkan untuk meningkatkan keamanan dengan melihat kebutuhan yang sesuai dengan keadaan jaringan yang ada, itu disebabkan karena disamping keamanan yang kita prioritaskan ada faktor-faktor lain seperti Performa, spesifikasi Jaringan, spesifikasi perangkat dan biaya yang Perlu diperhatikan. IPSec merupakan salah satu solusi untuk meningkatkan keamanan data pada jaringan komputer yang mendukung banyak metode otentikasi dan enkripsi. IPSec bekerja dengan melakukan enkripsi pada paket data secara otomatis sebelum dikirimkan. Dengan demikian walaupun data berhasil disadap oleh pihak ketiga maka data tidak akan berguna karena data telah terenkripsi. IPSec pun memeriksa integritas data dan keaslian sumber pengirim. Dan yang lebih penting adalah kemudahan dalam implementasi dengan tidak memerlukan prasyarat sistem yang tinggi dan mahal. Sehingga penguna komputer bisa berfikir kembali untuk segera melakukan pengamanan data.

Kata kunci: Keamanan jaringan, Keamanan data, IPSec.

PENDAHULUAN

Perkembangan dunia telekomunikasi saat ini sangat pesat seiring dengan eningkatan kebutuhan layanan yang cepat dan efisien. Begitu juga dengan komunikasi data, mulai dari koneksi antar dua computer hingga jaringan komputer. Jaringan komputer saat ini merupakan suatu layanan yang sangat dibutuhkan. Jaringan komputer mempunyai manfaat yang lebih dibandingkan dengan komputer yang berdiri sendiri. Jaringan komputer memungkinkan pemakaian secara bersama data, perangkat lunak dan peralatan. Sehingga kelompok kerja dapat berkomunikasi lebih efektif dan efisien [9].

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 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.

KAJIAN LITERATUR

TCP/IP (Transmission Control Protokol/Internet Protocol)

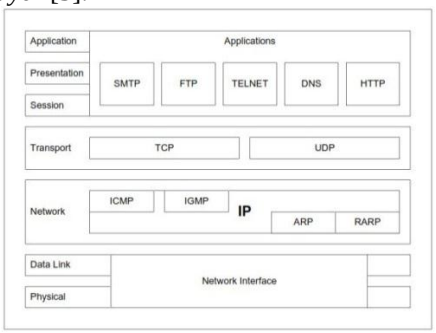
Protokol adalah spesifikasi formal yang mendefinisikan prosedur-prosedur yang harus diikuti ketika mengirim dan menerima data (Werner, 1996). Protokol mendefinisikan jenis, waktu, urutan dan pengecekan kesalahan yang digunakan dalam jaringan. *Transmission Control Protocol/Internet Protocol* (TCP/IP) merupakan protokol untuk mengirim data antar komputer pada jaringan. Protokol ini merupakan protokol yang digunakan untuk akses Internet dan digunakan untuk komunikasi global. TCP/IP terdiri atas dua protokol yang terpisah. TCP/IP menggunakan pendekatan lapisan (*layer*) pada saat membangun protokol ini. Dengan adanya pendekatan berlapis ini memungkinkan dibangunnya beberapa layanan kecil untuk tugas-tugas khusus [9].

TCP/IP terdiri dari lima layer, yaitu:

(a) Layer *Application*, di dalam layer ini aplikasi seperti FTP, Telnet, SMTP, dan NFS dilaksanakan.
(b) Layer *Transport*, di dalam layer ini TCP dan UDP menambahkan data transport ke paket dan melewatkannya ke layer *Internet*.
(c) Layer *Internet*, layer ini mengambil paket dari layer *transport* dan menambahkan informasi alamat sebelum mengirimkannya ke layer *network interface*.
(d) Layer *Network Interface*, di dalam layer ini data dikirim ke *layer physical* melalui *device* jaringan.
(e) Layer *Physical*, *layer* ini merupakan sistem kabel yang digunakan untuk proses mengirim dan menerima data.

TCP/IP dikirimkan ke setiap jaringan lokal sebagai subnet yang masing-masing subnet telah diberi alamat. IP yang menggunakan pengalamatan disebut dengan IP Address. IP Address ini digunakan untuk mengidentifikasi subnet dan host secara logik di dalam TCP/IP (Staff of Linux Journal, 2004).

TCP/IP dikembangkan mengacu pada model *Open System Interconnection* (OSI), dimana, *layer-layer* yang terdapat pada TCP tidak persis sama dengan *layer-layer* yang\ terdapat pada model OSI. Terdapat empat *layer* pada TCP/IP, yaitu: *network interface*, *network*, *transport* dan *application*. Tiga *layer* pertama
pada TCP/IP menyediakan *physical standards*, *network interface*, *internetworking*, dan fungsi *transport*, yang mengacu pada empat *layer* pertama pada model OSI. Tiga *layer* teratas dari model OSI direpresentasikan di model TCP/IP sebagai satu *layer*, yaitu *application layer* [3].



Gambar 1
TCP/IP dan OSI model

Internet Protocol Security (IPSec)

IPSec (IP Security) adalah sekumpulan standard dan protocol yang bertujuan untuk menyediakan keamanan dan kerahasiaan dalam pertukaran data di layer network.

IPSec didefinisikan oleh sebuah badan internasional bernama IETF (Internet Engineering Task Force), yang terdiri dari pada ilmuwan, praktisi, operator, dan vendor jaringan yang mempunyai misi untuk memajukan internet melalui penelitian dan pengembangan yang dilakukannya [4].

Dua teknik utama yang digunakan pada IPSec adalah Otentikasi dan Enkripsi. Otentikasi bertujuan untuk mengecek keaslian dari sumber atau pengirim paket data. Apakah benar sebuah paket dikirimkan dari sumber atau alamat IP seperti yang tertera di header paket atau jangan-jangan paket dikirim dari sumber yang dipalsukan (spoofing).

Teknik yang digunakan pada otentikasi juga berkhasiat untuk mengecek integritas dari paket data. Integritas data berarti paket yang diterima haruslah sama dengan paket yang dikirim, jangan sampai berbeda. Jika berbeda, maka ada kemungkinan paket tersebut telah diubah oleh seseorang atau sesuatu di tengah perjalanan sehingga paket tersebut tidak layak lagi untuk diterima.

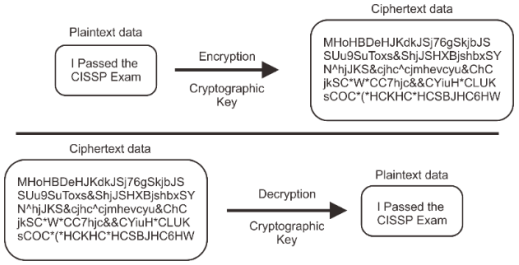
Teknik kedua pada IPSec adalah enkripsi, tujuannya untuk menjaga kerahasiaan (confidentiality) dari paket data yang dikirim.

Kerahasiaan disini artinya paket tersebut hanya boleh dibaca oleh penerima yang dituju. Cara menjaga kerahasiaan data adalah dengan melakukan enkripsi pada paket tersebut sebelum dikirimkan.

Jika paket yang sudah di-enkripsi jatuh ke tangan seseorang yang tidak berhak untuk menerima paket tersebut, maka paket tersebut tidak akan berguna bagi orang tersebut karena paket terenkripsi tidak akan bisa dibaca tanpa key enkripsi yang tepat. Paket terenkripsi hanya bisa dibuka dan dibaca oleh orang yang mempunyai key enkripsi untuk membukanya.

Enkripsi bekerja dengan cara mengubah data berbentuk teks biasa (cleartext atau plaintext) menjadi kode-kode acak yang tidak bisa dibaca, yang disebut ‘ciphertext’.

Proses perubahan ini menggunakan algoritma enkripsi dan kunci enkripsi (encryption key). Kunci enkripsi disebut juga kunci kriptografi (cryptographic key).

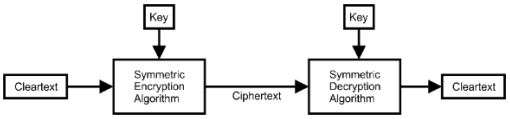


Gambar 2
Enkripsi dan Dekripsi

Terlihat pada gambar bahwa teks yang berbunyi "I Passed…" setelah mengalami proses enkripsi akan menjadi rangkaian teks yang tidak bisa dibaca dan dimengerti, bahkan oleh seorang super jenius sekalipun.

Disisi penerima, proses sebaliknya dilakukan yaitu proses dekripsi (decryption) dimana ciphertext yang tidak bisa dibaca dijadikan menjadi teks biasa kembali, dengan menggunakan algoritma dekripsi dan sebuah key kriptografi/enkripsi, dimana key untuk dekripsi tersebut bisa sama dengan key yang digunakan untuk enkripsi (disebut enkripsi simetris) atau berbeda dengan key yang digunakan untuk enkripsi (disebut metode Enkripsi Asimetris).

Enkripsi Simetris atau dikenal juga dengan nama lain seperti enkripsi Single Key, Shared Key, Secret Key, atau Private Key, adalah enkripsi yang menggunakan key yang sama untuk proses enkripsi dan proses dekripsi, seperti terlihat pada gambar berikut.



Gambar 3
Enkripsi Simetris

Terlihat bahwa baik pengirim maupun penerima menggunakan key enkripsi yang sama untuk melakukan proses enkripsi dan dekripsi pada paket data yang dikirimkan.

Algoritma enkripsi yang menggunakan teknik simetris antara lain : Twofish, Serpent, AES (Advanced Encrytion Standard), Blowfish, CAST5 (Carlisle Addams-Stafford Tavares 5), RC4 (Rivest Cipher 4), 3DES (Triple Data Encryption Standard) dan IDEA (International Data Encryption Algorithm).

Yang membedakan algoritma-algoritma ini adalah rumus perhitungan dan teknik pengacakan data yang dilakukan untuk menciptakan sebuah *ciphertext*.

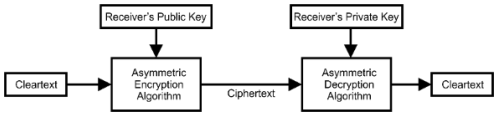
Sebagai contoh: AES menggunakan teknik substitusi dan permutasi dimana byte-byte data dipertukarkan dengan menggunakan sebuah table lookup, kemudian blok byte-byte data digeser atau ditukar posisinya dan setelah itu kolom-kolom data dicampur dan dikalikan dengan sebuah matrix yang berisi angka tertentu, sehingga menghasilkan sebuah ciphertext.

Contoh lainnya, RC4 menggunakan teknik permutasi dan rumus matematika yang diulang ratusan kali serta algoritma pengacakan dan pencampuran byte data yang cukup rumit untuk menghasilkan sebuah paket baru yang disebut 'pseuorandom stream of bits'.

Jenis-jenis algoritma yang berbeda ini bisa dianalogikan seperti resep ayam goreng dengan teknik masak dan bumbu yang berbeda, namun hasil akhirnya tetaplah ayam goreng.

Jenis enkripsi kedua selain enkripsi simetris adalah Enkripsi Asimetris atau disebut juga Enkripsi Public Key, yaitu teknik enkripsi yang menggunakan sepasang key yang disebut "public key" (untuk enkripsi) dan "private key" (untuk dekripsi).

Dalam sebuah komunikasi yang menggunakan enkripsi asimetris, masing-masing pihak yang terlibat harus mempunyai sepasang key tersebut. Jika sebuah paket di-enkripsi menggunakan Public Key yang dimiliki oleh user A, maka paket tersebut hanya bisa dibuka (di-dekripsi) dengan menggunakan Private Key yang dimiliki oleh user A. Tidak ada key lain diseluruh dunia yang bisa membuka paket tersebut.

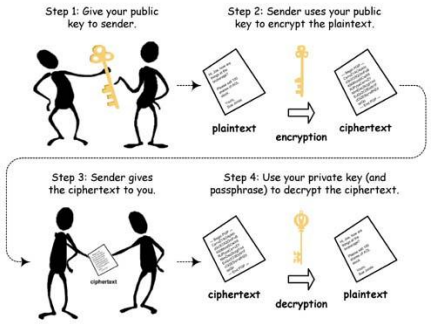


Gambar 4
Enkripsi Asimetris

Terlihat bahwa pengirim menggunakan public key dari penerima (receiver's public key) untuk melakukan enkripsi pada data yang akan dikirim. Setelah ciphertext sampai di tujuan, penerima akan menggunakan private key miliknya (receiver's private key) untuk melakukan dekripsi terhadap ciphertext tersebut agar bisa kembali menjadi data yang bisa dibaca. Berikut adalah gambar yang menunjukan langkah-langkah dalam melakukan enkripsi asimetris.

Langkah pertama menggunakan enkripsi asimetris adalah, penerima perlu memberitahukan public key-nya kepada orang yang akan mengirimkan data terenkripsi kepadanya.

Pengirim data lalu menggunakan public key dari penerima untuk melakukan enkripsi pada data yang akan dikirimnya. Sesampainya data, penerima akan menggunakan private key miliknya, sebagai satu-satunya keyyang bisa membuka paket tersebut, untuk melakukan dekripsi pada ciphertext yang diterima.



Gambar 5
Langkah-langkah Enkripsi Asimetris

Algoritma enkripsi yang menggunakan teknik Asimetris antara lain: Diffie-Hellman, DSS (Digital Signature Standard), ElGamal, Elliptic Curve, RSA (Rivest, Shamir, and Adleman), Paillier, Cramer-Shoup, dan YAK.

Sedangkan protokol dan aplikasi yang menggunakan enkripsi asimetris antara lain: PGP (Pretty Good Privacy), GPG (GNU Privacy Guard), IKE (Internet Key Exchange), ZRTP (Zimmermann Real-Time Transport Protocol), SSL (Secure Socket Layer), SILC (Secure Internet Live Conferencing), SSH (Secure Shell), Timekoin, dan Bitcoin.

Public key adalah *key* yang dipublikasikan kepada umum dan boleh dipakai oleh siapapun yang perlu mengirimkan data terenkripsi kepada anda, sedangkan private key adalah key rahasia yang tidak boleh diberitahukan kepada siapa pun.

Resiko akibat *public key* di-ekspose kepada umum adalah adanya kemungkinan penyerang menggunakan public key anda untuk membuat paket data terenkripsi dan kemudian mengirimkan paket tersebut kepada anda dengan mengaku sebagai orang yang anda kenal (memalsukan alamat sumber di header paket).

Untuk mengatasi serangan ini, diperlukan sebuah mekanisme untuk membuktikan keaslian dari sumber yang mengirimkan paket data terenkripsi.

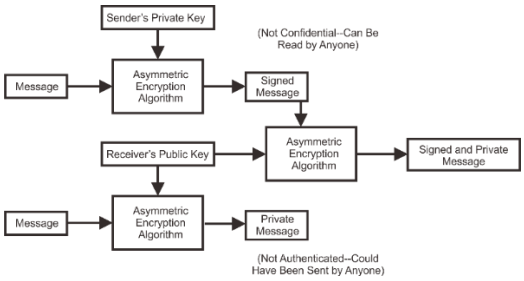
Enkripsi asimetris bisa digunakan untuk mengatasi hal ini, yaitu dengan membuat apa yang disebut "digital signature" atau tanda tangan digital.

Untuk membuat digital signature, pengirim harus melakukan enkrispsi sebanyak dua kali. Enkripsi pertama menggunakan private key dari pengirim untuk meng-enkripsi data cleartext. Hasil dari enkripsi tersebut di-enkripsi sekali lagi dengan public key dari penerima. Di sisi penerima, proses dekripsi juga menjadi dua kali, yaitu pertama dengan private key dari penerima dan kedua dengan public key dari pengirim.

Karena private key dari pengirim adalah bukti otentik bahwa paket tersebut dibuat oleh pengirim (pengirim adalah satu-satunya orang yang memiliki private key tersebut), maka paket yang dienkripsi menggunakan private key pengirim adalah bukti otentik bahwa paket tersebut adalah benar dari si pengirim.

Proses dimana pengirim melakukan enkripsi menggunakan private key miliknya sendiri disebut membuat "digital signature". Paket data yang dihasilkan disebut paket "signed" atau yang sudah ditandatangani (secara digital) oleh si pengirim.

Berikut adalah diagram yang menunjukan kemungkinan-kemungkinan yang bisa dilakukan dengan enkirpsi asimetris, dimana bisa dihasilkan tiga jenis data atau pesan ("message").



Gambar 6
Enkripsi Asimetris

Ketiga jenis data atau pesan tersebut adalah:

1. "Signed", paket dienkripsi 1 kali dengan private key dari pengirim, sehingga bisa dibuka oleh siapapun yang mempunyai *public key* pengirim.
   Sifat paket: Tidak confidential (bisa dibaca oleh siapa pun karena public key pengirim memang terbuka untuk dipakai oleh semua orang), tetapi terotentikasi (menunjukan paket tersebut benar-benar berasal dari pengirim yang valid karena pengirim adalah satu-satunya yang memiliki private key tersebut, kecuali private key tersebut bocor atau dicuri orang lain)

2. "*private*", paket dienkripsi 1 kali dengan *public key* dari penerima sehingga hanya bisa dibuka oleh penerima yang mempunyai pasangan private key yang cocok.
   Sifat paket: *Confidential* (hanya bisa dibuka oleh orang yang memegang *private key* yang merupakan pasangan dari *public key* yang dipakai untuk enkripsi), tetapi

tidak Terotentikasi (pengirim data bisa saja orang lain yang menyamar sebagai pengirim)

3. "*Signed and Private*", paket dienkripsi 2 kali dengan *private key* pengirim dan public key penerima.
   Sifat paket: *Confidential* (hanya bisa dibuka oleh penerima) dan Terotentikasi (terbukti bahwa paket berasal dari pengirim yang *valid* karena ada digital signature dari pengirim)

Aplikasi populer yang menggunakan IPSec adalah VPN (Virtual Private Network) yaitu jaringan *privat* terenkripsi yang dibuat melalui jaringan public yang tidak aman seperti internet. IPSec digunakan pada VPN untuk melakukan otentikasi dan enkripsi data [4].

Network Address Translation (NAT)

Seperti yang telah anda ketahui, keterbatasan alamat IP versi 4 adalah kendara yang sangat besar yang membuat tidak semua orang bisa terkoneksi ke internet. Solusi penghematan alamat IP dengan subnet mask tidaklah menyelesaikan masalah dan hanya menunda ledakan permasalahan akibat kurangnya alamat IP yang tersedia. Lalu apa yang harus dilakukan ?

Dengan NAT, anda tidak membutuhkan alamat IP publik karena NAT bisa melakukan konversi alamat private ke publik. Sebagai contoh, jaringan perkantoran anda memiliki dua computer yang menggunakan alamat IP 10.1.1.2 dan 10.1.1.3. Saat berlangganan internet, Anda hanya diberi sebuah alamat IP publik 202.152.0.2 yang tentu saja tidak bisa digunakan oleh kedua computer. Untuk mengatasi masalah ini, anda bisa menggunakan fungsi NAT yang pada contoh ini adalah sebuah router.

Pada mesin NAT (yang bisa berupa computer biasa), Anda harus memiliki dua interface untuk jaringan dimana interface yang satu akan terhubung dengan jaringan lokal yang dalam contoh kasus ini mendapatkan alamat IP 10.1.1.1 sedangkan interface yang satunya lagi akan diberikan alamat IP publik internet yang dalam contoh ini adalah 202.152.0.2.

Kini, saat computer 10.1.1.2 atau computer 10.1.1.3 ingin koneksi ke internet, permintaan mereka akan melalui NAT karena default gateway dari kedua computer ini telah disetting ke alamat 10.1.1.1 (maaf, tidak ada digambar karena saya yakin adnda telah faham). NAT akan merubah alamat IP baik dari 10.1.1.2 maupun 10.1.1.3 menjadi alamat IP publik 202.152.0.2 sehingga permintaan tersebut bisa bekerja di dalam jaringan internet.

Dengan NAT, Anda bisa men-sharing sebuah alamat IP publik untuk dipakai bersama-sama dan komputer yang bisa berbagi koneksi ini jumlahnya tidak terbatas. Jadi seperti yang saya katakana, dengan NAT, jumlah komputer yang terkoneksi ke internet menjadi tidak terbatas.

Masalah keterbatasan alamat IP bukan satu-satunya alasan orang menggunakan NAT. Betul sekali, masih ada fungsi lain dari NAT yang sangat berguna seperti masalah security atau keamanan. Dengan NAT, semua lalu lintas akan difilter terlebih dahulu sehingga paket-paket jahat bisa saja diblokir. Selain itu, dengan NAT, server-server di internet tidak akan bisa mengetahui secara pasti komputer mana yang telah mengakses dirinya sehingga NAT juga menjadi suatu metode untuk menyembunyikan diri.

NAT sendiri ada beberapa macam dan tidak hanya digunakan untuk membagi banyak alamat IP private menjadi satu alamat IP publik. Beberapa jenis NAT adalah SNAT, DNAT dan PAT yang akan kita bahas pada bagian ini.

SNAT (Statik Network Address Translation)

Suatu ketika, Anda sebagai seorang konsultan dimintai bantuan untuk menyelesaikan sebuah kasus unik. Sebuah perusahaan tidak kekurangan alamat IP publik sama sekali namun ingin tetap menggunakan NAT untuk melindungi host yang berada didalam jaringan. Mereka memiliki dua komputer dengan alamat 10.1.1.2 dan 10.1.1.3 dan mendapatkan dua alamat IP publik yaitu 202.152.0.2 dan 202.152.0.3.

Mereka ingin agar komputer 10.1.1.2 saat akses ke internet selalu menggunakan alamat ip 202.152.0.2 sedangkan alamat IP 10.1.1.3 saat akses ke internet selalu menggunakan alamat IP 202.152.0.3. Dsini. Tidak ada alamat IP publik yang disharing, dan yang anda butuhkan disini adalah SNAT (Statik Network address Translation).

SNAT dikatakan statik karena alamat IP lokal selalu mendapatkan alamat IP publik yang sama. SNAT sering digunakan untuk melindungi server-server yang bisa diakses oleh publik seperti email server, web server dan server-server lainnya.

DNAT (Dynamic Network Address Translation)

Berbeda sedikit dengan SNAT adalah DNAT yang merupakan singkatan dari Dynamic Network Address Translation. Client anda kembali meminta bantuan kepada anda sebagai seorang konsultan jaringan yang

handal. Permasalahan muncul ketika ada sebuah komputer baru lagi yang juga membutuhkan koneksi ke internet sehingga total komputer yang hendak koneksi ke internet ada tiga sedangkan alamat IP publik yang tersedia hanya ada dua alisa kurang. Permsalahan semakin kompleks ketika ISP meminta bayaran tinggi untuk alamat IP statik tambahan karena terbatasnya alamat IP ini.

Solusi untuk kasus semacam ini adalah DNAT. Sesuai dengan namanya, DNAT akan menerjemahkan suatu alamat ke alamat lainnya yang ada didalam pool. Biar jelas, lihat contoh ini, yaitu 10.1.1.2, 10.1.1.3 dan 10.1.1.4 sedangkan anda hanya memiliki dua alamat publik yaitu 202.152.0.2 dan 202.152.0.3. Dengan SNAT, jelas alamat publik yang tersedia kurang namun dengan DNAT, alamat ini jumlah yang tidak sama ini tidaklah bermasalah. Saat komputer 10.1.1.2, 10.1.1.3 atau 10.1.1.4 terhubung ke internet, alamat IP yang digunakan akan dipilih secara acak , antara 202.152.0.2 dan 202.152.0.3.

Akibat cara kerja yang begini, alamat IP publik yang digunakan oleh sebuah komputer lokal bisa berubah–ubah dan tidak tetap [10].

Firewall

Firewall adalah sebuah sistem atau kelompok sistem yang menerapkan sebuah access control policy terhadap lalu lintas jaringan yang melewati titik-titik akses dalam jaringan. Tugas firewall adalah untuk memastikan bahwa tidak ada tambahan diluar ruang lingkup yang diizinkan. *Firewall* bertanggung jawab untuk memastikan bahwa *acces control policy* yang diikuti oleh semua pengguna di dalam jaringan tersebut. Firewall sama seperti alat-alat jaringan lain dalam hal untuk mengontrol aliran lalu lintas jaringan. Namun, tidak seperti alat-alat jaringan lain, sebuah firewall harus mengontrol lalu lintas network dengan memasukkan faktor pertimbangan bahwa tidak semua paket-paket data yang dilihatnya adalah apa yang seperti terlihat. Firewall digunakan untuk mengontrol akses antara network internal sebuah organisasi Internet. Sekarang ini firewall semakin menjadi fungsi standar yang ditambahkan untuk semua host yang berhubungan dengan network (Purbo, 2000) [9].

Fungsi-fungsi umum firewall adalah sebagai berikut:

1. *Static packet filtering* (penyaringan paket secara statis)
2. Dynamic packet filtering (penyaringan paket secara dinamis)
3. Stateful filtering (penyaringan paket berdasarkan status)
4. Proxy

Microsoft Windows

Microsoft Windows atau yang lebih dikenal dengan sebutan Windows adalah keluarga sistem operasi. yang dikembangkan oleh Microsoft, dengan menggunakan antarmuka pengguna grafis.
Sistem operasi Windows telah berevolusi dari MS-DOS, sebuah sistem operasi yang berbasis modus teks dan command-line. Windows versi pertama, Windows Graphic Environment 1.0 pertama kali diperkenalkan pada 10 November 1983, tetapi baru keluar pasar pada bulan November tahun 1985, yang dibuat untuk memenuhi kebutuhan komputer dengan tampilan bergambar. Windows 1.0 merupakan perangkat lunak 16-bit tambahan (bukan merupakan sistem operasi) yang berjalan di atas MS-DOS (dan beberapa varian dari MS-DOS), sehingga ia tidak akan dapat berjalan tanpa adanya sistem operasi DOS. Versi 2.x, versi 3.x juga sama. Beberapa versi terakhir dari Windows (dimulai dari versi 4.0 dan Windows NT 3.1) merupakan sistem operasi mandiri yang tidak lagi bergantung kepada sistem operasi MS-DOS. Microsoft Windows kemudian bisa berkembang dan dapat menguasai penggunaan sistem operasi hingga mencapai 90%.

Dimulai dari DosShell for DOS 6 buatan Microsoft dan inginnya Microsoft bersaing terhadap larisnya penjualan Apple Macintosh yang menggunakan GUI, Microsoft menciptakan Windows 1.0 Nama ini berasal dari kelatahan karyawan Microsoft yang menyebut nama aplikasi tersebut sebagai Program Windows (Jendela Program). Windows versi 2 adalah versi Windows pertama yang bisa diinstal program. Satu-satunya program yang bisa ditambahkan adalah Microsoft Word versi 1. Windows versi 3 menjanjikan aplikasi tambahan yang lebih banyak, kelengkapan penggunaan, kecantikan user interface atau antarmuka dan mudahnya konfigurasi. Windows versi 3.1 adalah versi Windows yang bisa mengoptimalisasi penggunaannya pada prosesor 32-bit Intel 80386 ke atas. Windows versi 3.11 adalah versi Windows terakhir sebelum era Start Menu. Windows 3.11 pun adalah versi Windows pertama yang mendukung networking/jaringan. Versi Hibrida dapat dijalankan tanpa MS-DOS. Versi Hibrida tersebut menginstalasi dirinya sendiri dengan DOS 7. Tidak seperti Windows versi 16-bit yang merupakan shell yang harus diinstalasi

melalui DOS terlebih dahulu. Aplikasinya pun berbeda. Meskipun Windows 9X dapat menjalankan aplikasi Windows 16-bit, namun Windows 9X memiliki grade aplikasi sendiri - X86-32, Windows 9X sangat terkenal dengan BSOD (Blue Screen of Death) [5].

Implementasi IPSEC

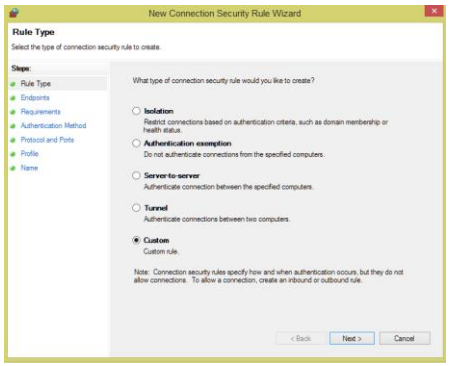
Ketika akan mengimplementasikan IPSec, hal yang penting untuk diketahui adalah adanya suatu keseimbangan antara mengamankan data dari user yang tidak berhak dan membuat user yang punya akses untuk dapat masuk ke dalam jaringan. Untuk itulah, hal yang perlu dilakukan adalah dengan melakukan analisis resiko 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 [8].

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

1. 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.
2. 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.
3. 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 Security) memberikan level keamanan tingkat tinggi.

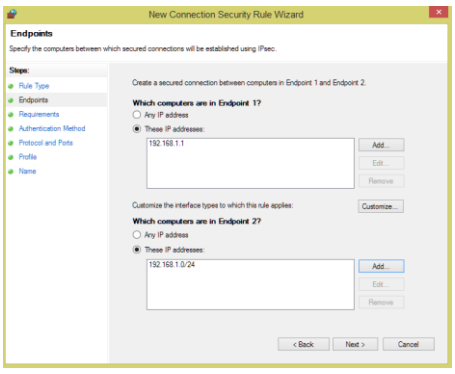
Adapun langkah-langkah untuk implementasi IPSec pada komputer server Microsoft Windows adalah sebagai berikut:

1. Langkah pertama buka ***Windows Firewall*** dengan ***Advanced Security*.**
2. Klik kanan ***Connection Security Rules*** dan pilih ***New Rule.***
3. Pilih ***Custom*** sebagai rule type lalu klik ***next.***



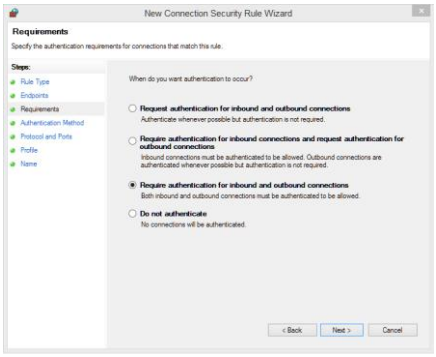
Gambar 7
***New Connection* IPSec**

4. Masukan alamat IP server pada bagian daftar alamat pada **"*Which computers are in Endpoint1*?"** dan IP client pada bagian daftar alamat pada **"*Which computers are in Endpoint2*?".** Alamat IP bisa berupa range atau subnet. lalu pilih ***Next*** untuk melanjutkan.



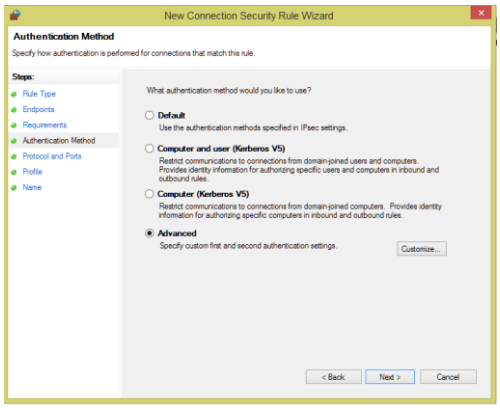
Gambar 8
***Input* IP *Endpoint* pada IPSec**

5. Pilih ***Require authentication for inbound* and outbound *connections*** lalu ***Next***.



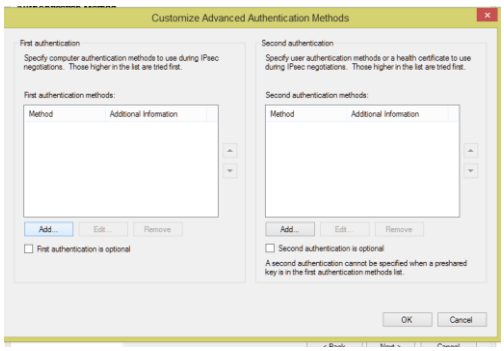
Gambar 9
Otentikasi pada IPSec

6. Klik ***Customize*** pada pilihan ***Advanced***



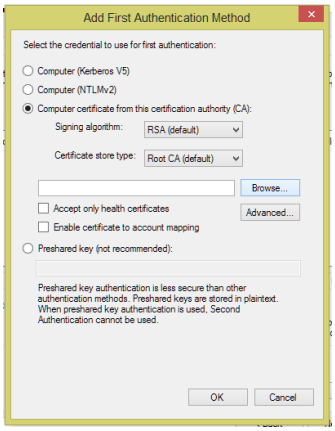
Gambar 10
Metode Otentikasi

7. Klik ***Add*** pada ***First Authentication***



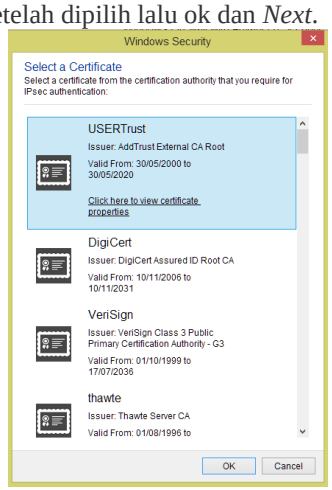
Gambar 11
Kostumisasi metode otentikasi

8. Pilih ***computer certificate from this certification authority*** **(CA),** lalu klik *browse* untuk memilih CA.



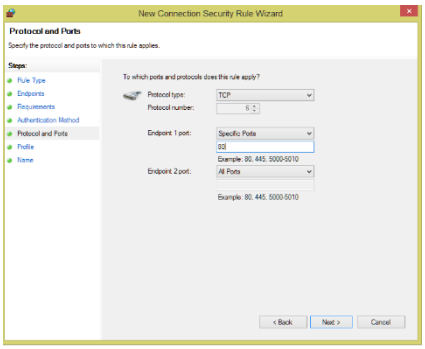
Gambar 12
Memilih metode otentikasi

9. Setelah dipilih lalu ok dan *Next*.



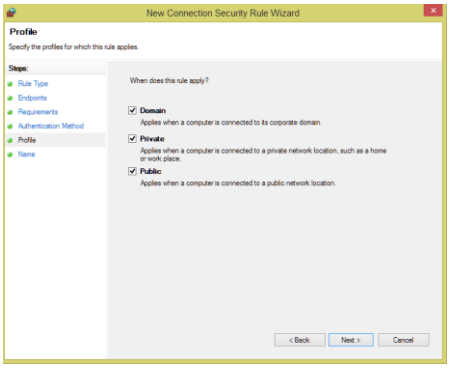
Gambar 13
Memilih *Certification authority*

10. Lalu tentukan *protocol* dan *port*,



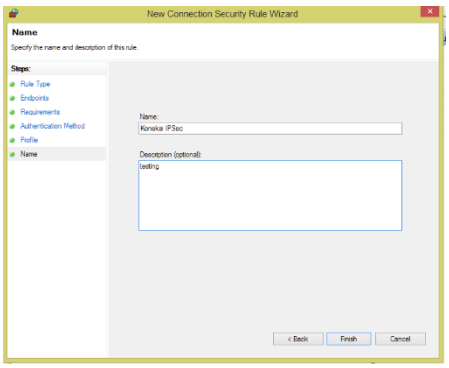
Gambar 14
Menentukan Protokol dan *Port*

11. Pilih semua ***profile rule*** lalu ***Next***.



Gambar 15
Memilih *Profiles Rule*

12. Masukan nama dan deskripsi dari rule yang telah dibuat, lalu klik ***Finish*** untuk mengakhiri langkah konfigurasi.

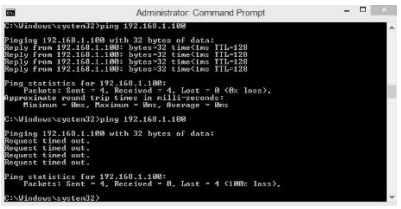


Gambar 16
Menentukan nama dan deskripsi rule

Langkah selanjutnya adalah konfigurasi pada komputer *client* dengan mengulangi langkah "a" sampai "l" sama persis.

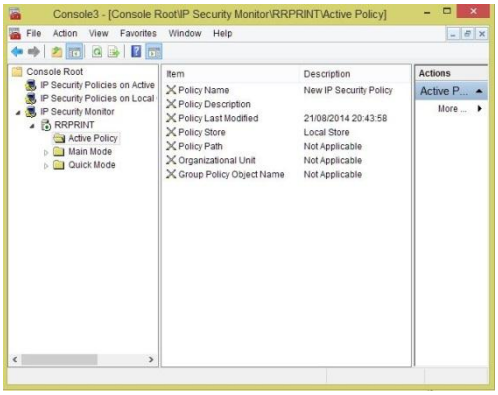
PEMBAHASAN

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 17
Koneksi jaringan

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



Gambar 18
IPSec Monitor

PENUTUP

Penelitian ini fokus dalam menganalisa dan mengeskplorasi fitur keamanan jaringan dalam Microsoft windows. Microsoft windows dapat memenuhi kebutuhan sistem dalam mengimplementasikan IPSec tanpa membutuhkan tambahan perangkat lunak lain sehingga lebih efisien dan dapat menghindari penggunaan banyak aplikasi dalam sebuat desain sistem keamanan jaringan.

Dengan menggunakan IPSec 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.

IPSec dapat diimpelentasikan dalam berbagai kasus baik dalam model jaringan client server seperti contoh diatas ataupun

model jaringan point to point dengan memanfaatkan fitur tunnel dalam IPSec.

REFERENSI

[1] Ahmad, N. M., & Yaacob, A. H. (2012). IPSec Over Heterogeneous IPv4 and IPv6 Network: Issues And Implementation. *International Journal of Computer Networks & Communications (IJCNC) Vol.4, No.5*, 57-72.

[2] Asari, M. H., & Nurryna, A. F. (2012). Pemblokiran Akses Informasi Elektronik dan Dokumen Elektronik yang Memiliki Muatan yang Melanggar Kesusilaan Di Warung Internet Salwanet Sragen. *Indonesian Journal on Network and Security (IJNS), Volume 1 Nomor 1, ISSN : 2302-5700*, 67-73.

[3] Asnawati. (2009). Analisa interkoneksi INTERNET PROTOCOL SECURITY (IPSEC) pada jaringan berbasis NETWORK ADDRESS TRANSLATION (NAT). *Media Infotama, Volume 4, No.8*, 76-85.

[4] Hidayat, J. (2014). *CEH : 500% Illegal.* Jakarta: JASAKOM.

[5] wikipedia. (2014, Juni 30). *wikipedia*. Retrieved from wikipedia: http://id.wikipedia.org/wiki/Microsoft_Windows

[6] binushacker. (2013, April 13). *yudha.binushacker.net* Retrieved from binushacker : http://yudha.binushacker.net/2013/04/fitur-keamanan-pada-windows-8.html

[7] Muslim , M. A. (2007). Analisa Teknis Perbandingan Router Linux dengan Router Mikrotik pada Jaringan Wireless. *Jurnal Teknologi Informasi DINAMIK Volume XII, No.1, ISSN : 0854-9524*, 10-21.

[8] Noertjahyana, A., & Adipranata, R. (2005). IPSEC sebagai salah satu solusi keamanan data pada jaringan komputer. *Seminar Nasional Aplikasi Teknologi Informasi 2005 (SNATI 2005), ISBN: 979-756-061-6*, (pp. 111-115). Yogyakarta.

[9] Riadi, I. (2011). Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik. *JUSI Vol 1, No.1, ISSN: 2087-8737*, 71-80.

[10] S'to. (2014). *Networking+ : 100% iLLEGAL.* Jakarta: JASAKOM.