OPTIMASI KEAMANAN JARINGAN KAMPUS MENGGUNAKAN *SYNCHRONOUS PROCESSING TECHNOLOGY BASED ON HARDWARE* DAN IP SEC

Oleh

Slamet
Information System Department
Institut Bisnis dan Informatika Stikom Surabaya, Indonesia
slamet@stikom.edu

Abstrak

Jaringan komputer memainkan peran penting dalam hal pengajaran, penelitian, manajemen dan proses bisnis di kampus. Untuk membuat jaringan kampus lebih aman dan stabil, universitas biasanya menginvestasikan sejumlah dana yang cukup besar untuk membeli sejumlah perangkat keamanan dan perangkat lunak untuk digunakan jaringan kampus. Perangkat keamanan dan perangkat lunak terutama digunakan untuk menjaga serangan eksternal dan melindungi serta mengontrol keamanan jaringan di lingkungan internal. Sementara penggunaan perangkat keras dan perangkat lunak keamanan ini sering digunakan dalam kerangka yang sederhana, tanpa koneksi satu sama lain, dan tidak membentuk sistem pertahanan terpadu, sehingga investasi besar tidak dapat berperan dalam menjaga keamanan. Paper ini bermaksud untuk memperkenalkan ide keamanan jaringan secara global dan membentuk sistem pertahanan terpadu menggunakan *Synchronous Processing Technology Based on Hardware* (SPOH) untuk menangani masalah keamanan jaringan. Selain itu, ditambahkannya IPSec dapat meningkatkan keamanan data pada jaringan komputer yang mendukung banyak metode otentikasi dan enkripsi. IPSec melakukan enkripsi pada paket data secara otomatis sebelum dikirimkan. Dengan demikian walaupun data berhasil disadap oleh pihak ketiga maka data tidak dapat dibuka karena data telah terenkripsi. IPSec memeriksa integritas data dan keaslian sumber pengirim. Dan yang lebih penting adalah kemudahan dalam implementasi dengan tidak memerlukan prasyarat sistem yang tinggi dan mahal. Dengan demikian, SPOH dan IPSec dapat mengoptimasi keamanan pada jaringan kampus.

Kata kunci: Keamanan jaringan, Keamanan data, SPOH, IPSec.

1. PENDAHULUAN

Perkembangan teknologi informasi secara terus-menerus membutuhkan infrastruktur jaringan kampus terus berkembang dan lebih sempurna. Sistem pengajaran, penelitian dan proses bisnis perkantoran, telah menjadi semakin tergantung pada jaringan. Dengan terus berkembangnya teknologi jaringan, berbagai masalah keamanan mulai muncul. Menghilangkan masalah keamanan jaringan telah dan terus menjadi fokus untuk memperbaiki informasi di kampus. Dalam situasi keamanan yang serius ini diperlukan optimasi sistem keamanan jaringan kampus. Optimasi sistem keamanan jaringan kampus bertujuan untuk mengelola pengguna internal secara efektif, melalui otentikasi keamanan jaringan, perlindungan agar komputer selalu sehat, dan sebagainya. Melalui serangkaian tindakan, identitas pengguna dalam jaringan dapat dipantau secara legal. Keamanan

internet dan kesehatan komputer dapat dijaga, keamanan komunikasi dan standarisasi perilaku akses jaringan pengguna juga dapat dipantau.

Saat ini, langkah-langkah defensif untuk menjaga serangan eksternal menjadi cara yang masuk akal, tetapi tidak memuaskan digunakan dalam mempertahankan insiden keamanan jaringan secara internal. Untuk itu, cara membuat jaringan internal yang aman, stabil, dan andal telah menjadi fokus masalah yang perlu diselesaikan saat ini. Keamanan jaringan kampus saat ini terutama menghadapi masalah dan tantangan berikut:

a. Jaminan keamanan perangkat. Dalam insiden keamanan jaringan internal, tampak kecenderungan penyerangan terhadap server internal, penyerangan perangkat jaringan dan peralatan jaringan, khususnya perangkat inti jaringan. Hal ini menyebabkan perangkat menjadi *crash, restart* dan utilisasi CPU peralatan 100% dan masalah serius yang lainnya, sehingga terjadi gangguan komunikasi seluruh jaringan.
b. Manajemen keamanan peralatan. Karena ukuran jaringan yang meningkat, terpusat dan manajemen secara *remote* untuk perangkat jaringan telah menjadi cara umum manajemen jaringan. Namun, teknik manajemen tradisional dalam manajemen informasi seperti *username, password* dan segmen kunci lainnya dalam jaringan ditransmisikan dalam *clear text*, mudah dicuri, sehingga peretas mudah mengakses dan mengontrol peralatan, mengubah konfigurasi perangkat, dan menghasilkan gangguan pada aplikasi jaringan. Oleh karena itu, manajemen keamanan terhadap perangkat jaringan merupakan masalah penting lainnya yang perlu dipertimbangankan.

2. KAJIAN SISTEM MANAJEMEN KEAMANAN KAMPUS

2.1. Sistem Keamanan Jaringan Global

Sistem Keamanan Jaringan Keamanan Global [1] dijelaskan dalam beberapa bagian utama seperti Pusat Manajemen Kebijakan Keamanan, *Platform* Manajemen Keamanan, *Security Event Parser,* dan keamanan komputer klien.

2.1.1 Pusat Manajemen Kebijakan Keamanan

Pusat Manajemen Kebijakan Keamanan adalah komponen opsional sebagai solusi keamanan jaringan global, terkait pendistribusian keamanan jaringan atau kebijakan manajemen keamanan yang perlu ditempatkan secara terpusat. Informasi tentang identitas dari seluruh pengguna atau grup, informasi *host*, informasi jaringan, informasi perangkat lunak dan informasi lainnya dikelola melalui server pusat. Lebih penting lagi, Administrator dapat mengembangkan kebijakan keamanan pribadi melalui sistem terpusat dari manajemen kebijakan keamanan untuk menjamin integritas dari keseluruhan kelompok dalam strategi keamanan, sehingga terdapat operasional manajemen terpadu. Sementara itu, dilakukan desentralisasi manajemen keamanan server pada kampus cabang agar dapat mengelola diri sendiri, sedangkan manajemen jaringan pusat bertanggung jawab untuk sinkronisasi dan pengumpulan informasi.

2.1.2 *Platform* Manajemen Keamanan

Platform manajemen keamanan adalah otak atau komandan dari seluruh solusi keamanan jaringan global. *Platform* manajemen keamanan menyimpan informasi identitas pengguna. Sebelum pengguna mengakses jaringan secara formal, pengguna harus lulus otentikasi dengan menggunakan *platform* manajemen keamanan, untuk melindungi legitimasi identitas pengguna. Sementara itu, *platform* manajemen keamanan terhubung dengan keamanan klien. Hal ini untuk mendapatkan status keamanan PC dalam menghubungkan jaringan, sehingga dapat mengembangkan strategi keamanan yang sesuai dan integritas *host* sesuai dengan isu kebijakan keamanan. Dalam manajemen keamanan jaringan, terhubungnya *platform* manajemen keamanan dengan peralatan deteksi intrusi dapat melakukan perawatan efektif terkait sumber serangan. Selain itu dapat mencapai manajemen yang efektif untuk serangan jaringan, dan pada saat yang sama, mencegah serangan ARP dengan bekerja sama dengan gateway dan *inteligent* switch yang berfungsi sebagai pengamanan.

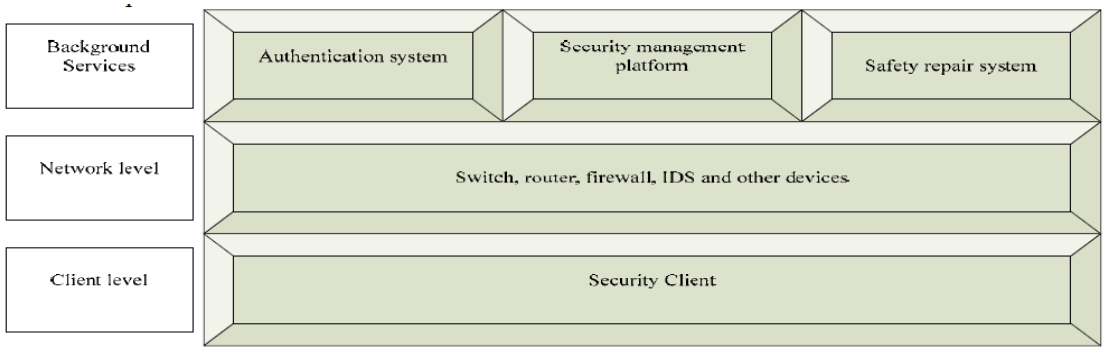
2.1.3 *Security Event Parser*

Peran *Security Event Parser* adalah mengumpulkan, menganalisis, dan melaporkan peristiwa keamanan. Di dalam *Security Event Parser* terdapat peralatan deteksi intrusi dan *data base* insiden keamanan sehingga dapat digunakan untuk menganalisa insiden keamanan secara akurat. *Feed back* dari deteksi intrusi ini untuk menentukan pelaporan ke server Manajemen Keamanan.

2.1.4 Keamanan Komputer Klien

Keamanan Klien terdapat PC klien yang *user-friendly*, perannya adalah untuk menyelesaikan otentikasi identitas pengguna, memeriksa integritas host, mengeluarkan kebijakan keamanan, dan menerima strategi perawatan dari manajemen keamanan ketika insiden keamanan terjadi. Sementara itu, bekerja sama dengan gateway keamanan dan platform manajemen keamanan, Keamanan Klien adalah alat yang berada pada sisi *host* yang digunakan untuk mencegah penyalahgunaan ARP.

Platform manajemen keamanan terpadu [2] arsitektur khusus yang ditunjukkan pada Gambar 1, terdiri dari tiga tingkat dan lima bagian:



Gambar. 1. Arsitektur Manajemen Keamanan Terpadu

2.2. Sistem Manajemen Keselamatan Peralatan Jaringan

Sistem manajemen keamanan peralatan jaringan terdiri dari keamanan fisik, keamanan *inteligent* switch, keamanan *firewall* dan keamanan peralatan deteksi intrusi.

2.3. Sistem Manajemen Arsitektur SO

Sistem Operasi Microsoft Windows adalah sistem operasi yang paling banyak digunakan, namun masih banyak celah yang harus dihilangkan. Solusi keamanan jaringan dilakukan dengan menghubungkan sistem operasi komputer dengan server Microsoft sehingga sistem operasi dapat mendeteksi, mengunduh, menginstall sistem keamanan untuk klien Windows. Seluruh proses berjalan secara otomatis tanpa atau melibatkan partisipasi pemakai.

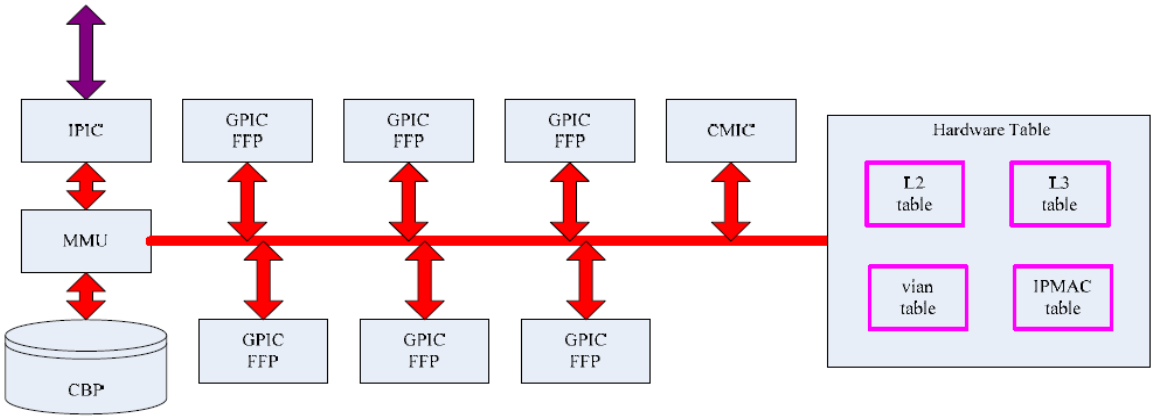
3. Metode Sistem Manajemen Keamanan Jaringan Kampus

Solusi keamanan jaringan kampus berfokus pada fitur keamanan pada seluruh peralatan jaringan sehingga dapat mencapai perlindungan keamanan jaringan di level *hardware*. *Hardware* sebagai inti dari suatu akses harus diperlakukan dengan hati-hati. Kemudian diimplementasikan protokol IPSec agar dalam pertukaran data di *layer* network menjadi aman dan rahasia.

3.1. Teknologi *Synchronous Processing Technology Based on Hardware*

Di dalam peralatan jaringan tradisional, keamanan dan kinerja selalu menjadi kontradiksi. Terlalu banyak pengaturan keamanan dapat meningkatkan sumber daya. Sehingga untuk melindungi keamanan diperlukan banyak sumber daya, yang mana akan mempengaruhi efisiensi operasional peralatan jaringan.

Dengan menggunakan teknologi *Synchronous Processing Technology Based on Hardware* (SPOH) [3] dapat meningkatkan independensi FFP (*Fast Filter Processor*) dimana akan dicapai perlindungan dan keamanan secara intelijen. Modul yang digunakan adalah *hardware* ASIC *chip* pada setiap *port*, sehingga setiap *port* dapat memproses *hardware* secara bersamaan dan tidak mempengaruhi kinerja keseluruhan. Prinsip-prinsip SPOH ditunjukkan pada gambar 2.



Gambar 2. Prinsip-prinsip Teknis SPOH

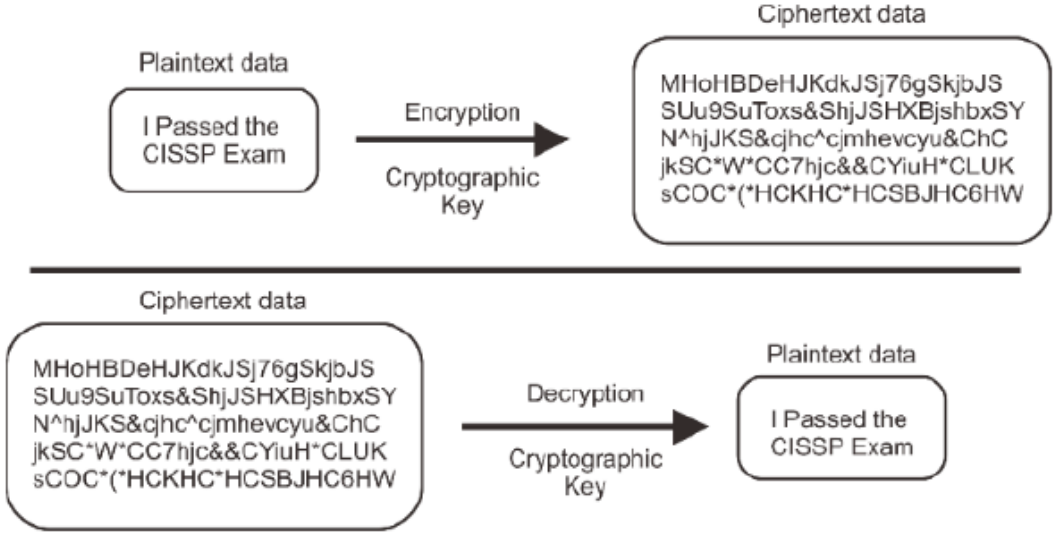
Dengan teknologi SPOH, manajemen keamanan dikirim kepada setiap *port* sehingga CPU bekerja secara *independent*. Beban CPU yang efektif tidak hanya membuat peralatan lebih aman tetapi juga menjaga stabilitas peralatan. Setelah menggunakan teknologi SPOH, kinerja keamanan jaringan menjadi seimbang.

3.2. IP SEC (IP Security)

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 untuk mengecek integritas dari paket data.

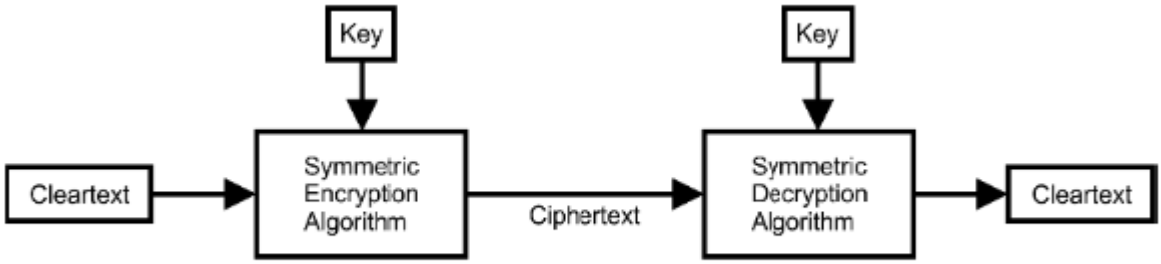
Teknik kedua pada IPSec adalah enkripsi, tujuannya untuk menjaga kerahasiaan (*confidentiality*) dari paket data yang dikirim. Kerahasiaan disini artinya paket tersebut hanya boleh dibaca oleh penerima yang dituju. Cara menjaga kerahasiaan data adalah dengan melakukan enkripsi pada paket tersebut sebelum 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 3 Enkripsi dan Dekripsi

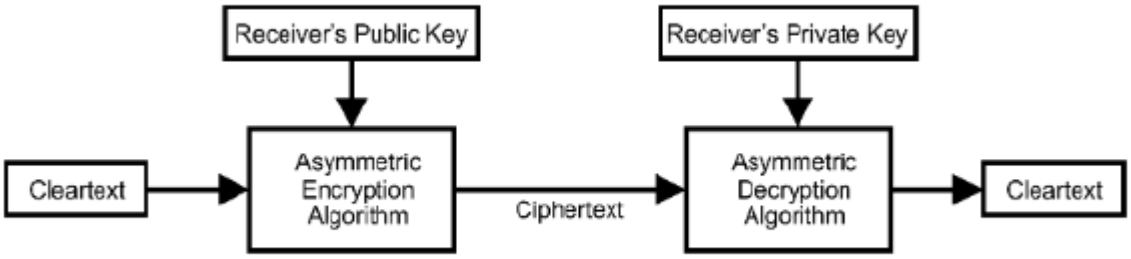
Pada gambar 3, bahwa teks yang berbunyi "I Passed…" setelah mengalami proses enkripsi akan menjadi rangkaian teks yang tidak bisa dibaca dan dimengerti. Di sisi penerima, proses sebaliknya dilakukan yaitu proses dekripsi (*decryption*) dimana *ciphertext* yang tidak bisa dibaca dijadikan menjadi teks 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 4.



Gambar 4. Enkripsi Simetris

Pada 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 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.



Gambar 5. Enkripsi Asimetris

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. Gambar 5 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 key yang bisa membuka paket tersebut, untuk melakukan dekripsi pada *ciphertext* yang diterima.

4. Implementasi IPSEC pada Jaringan Kampus

Dalam mengimplementasikan IPSec, hal terbaik adalah dengan memberikan hak akses *user* terhadap sumber daya hanya sebatas pada kepentingannya serta memastikan bahwa *user* melakukan akses terhadap suatu sumber daya secara aman dan efisien [5].

Terdapat tiga tingkatan level keamanan dalam implementasi kebijakan keamanan dengan menggunakan IPSec, 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 Security)* memberikan level keamanan tingkat tinggi.

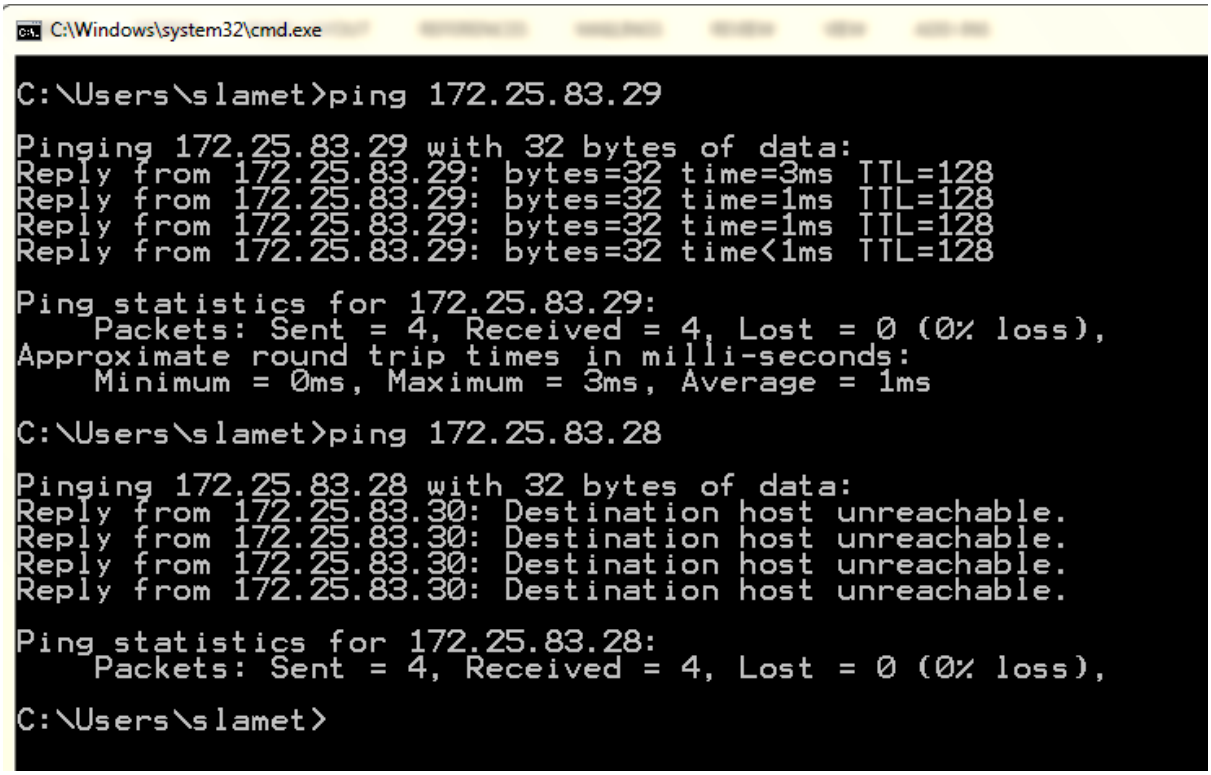
Adapun langkah-langkah untuk implementasi IPSec pada komputer server Microsoft Windows adalah sebagai berikut:

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.***
4. Masukkan 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 dapat berupa range atau subnet. lalu pilih ***Next*** untuk melanjutkan.
5. Pilih ***Require authentication for inbound*** **and outbound** ***connections*** lalu ***Next***.
6. Klik ***Customize*** pada pilihan ***Advanced***
7. Klik ***Add*** pada ***First Authentication***
8. Pilih ***computer certificate from this certification authority*** **(CA),** lalu klik *browse* untuk memilih CA.
9. Setelah dipilih lalu ok dan ***Next***.
10. Lalu tentukan ***protocol*** dan ***port***,
11. Pilih semua ***profile rule*** lalu ***Next***.
12. Masukan nama dan deskripsi dari *rule* yang telah dibuat, lalu klik ***Finish*** untuk mengakhiri langkah konfigurasi

Langkah selanjutnya adalah melakukan konfigurasi dengan mengulangi langkah “1” sampai “l2” pada komputer klien.

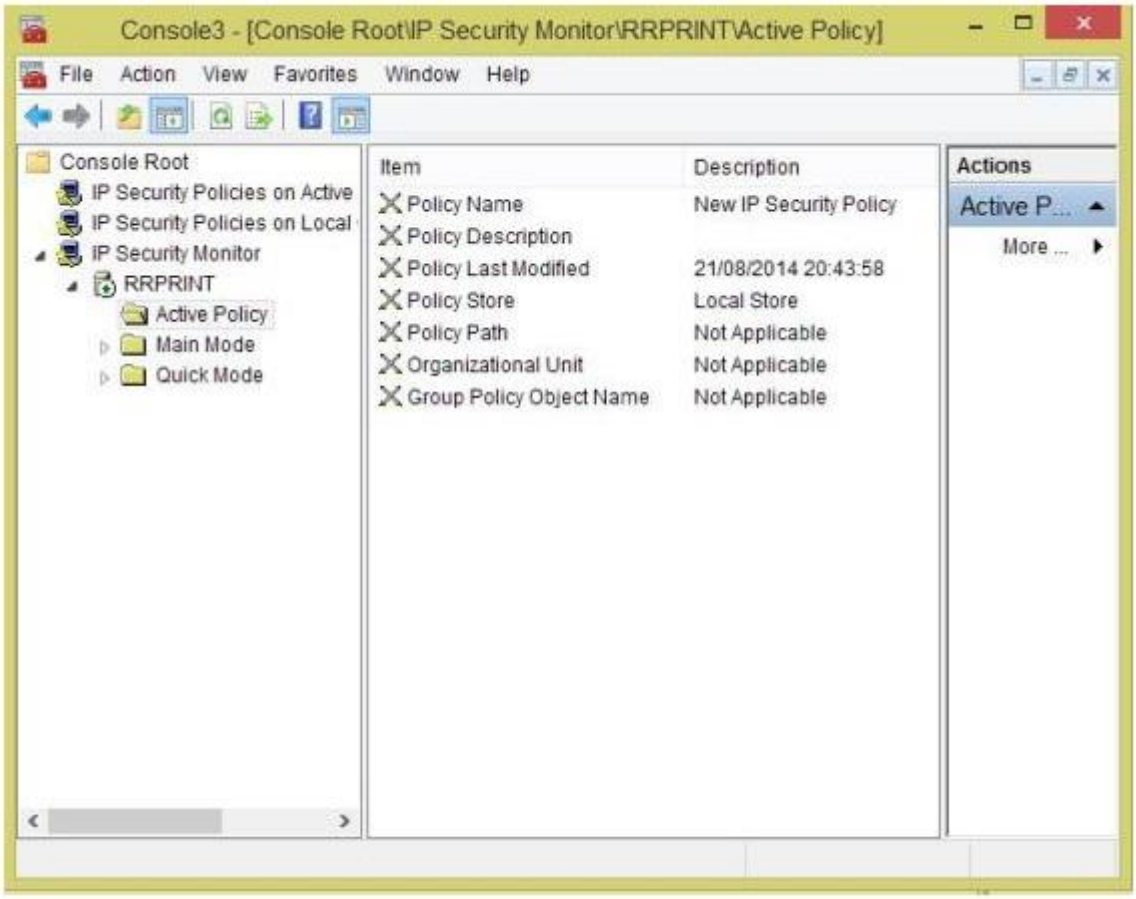
5. Pembahasan

Setelah semua tahapan dalam implementasi SPOH dan IPSec sudah dilakukan, maka perlu dilakukan pengamatan untuk memastikan bahwa manajemen keamanan ini dapat berjalan dengan baik. Cara termudah yang dapat dilakukan adalah dengan menggunakan *command ping* untuk melakukan verifikasi terhadap komunikasi.



Gambar 6. Test 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 7. Monitoring menggunakan IPSec

6. Kesimpulan

Penelitian ini bertujuan untuk memecahkan masalah keamanan jaringan dengan pembentukan manajemen keamanan jaringan kampus.

a. Pertama dengan mendesain hubungan jaringan dari komponen keamanan jaringan dan perlindungan secara keseluruhan termasuk keterkaitan perangkat keras dan perangkat lunak, pengaturan identitas *user* dan sudut pandang lain dari pemantauan keamanan jaringan.
b. Pada saat yang sama, melalui jaringan terdistribusi dan manajemen terpusat dapat membantu *user* untuk mencapai manajemen keamanan jaringan dalam mengimplementasikan model baru yang lebih baik.
c. Percobaan dilakukan dengan menganalisa dan mengeskplorasi fitur keamanan jaringan dalam Microsoft Windows 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 dapat meningkat karena IPSec melakukan enkripsi terhadap data yang dikirim pada jaringan tersebut.
d. Selain itu implementasi IPSec dapat dilakukan dengan mudah karena tidak memerlukan keahlian khusus yang harus dimiliki Administrator Jaringan.

Daftar Pustaka

[1] Xiaohua Li, *Network Security Management of University Research and Practice*, Science and Technology Innovation Herald, Zhejiang University. 2009

[2] Qunhui Ye, *Research about integrate solution of campus network security*, SCIENCE & TECHNOLOGY INFORMATION, Fujian Vocational and Technical College. (2010)

[3] Ruijie Networks, *Hardware-based Synchronous Processing — SPOH technology*, https://www.ruijienetworks.com/solutions/1261, China. 2018

[4] Rosyidina Safitri, *Implementasi dan Analisa Perbandingan QoS pada Jaringan VPN Berbasis MPLS menggunakan Routing Protocol RIPv2, EIGRP dan OSPF terhadap Tunneling IPsec untuk Layanan IP-Based Video Conference*, Universitas Indonesia. Jakarta. 2010

[5] Erwin R. & Irwan S., *Analisis dan Implementasi IPSec (Internet Protocol Security) OpenSwan dan OpenVPN (Virtual Private Network) pada Digital Payment*, Universitas Kristen Satya Wacana, Salatiga. 2016