PEMANFAATAN SMS GATEWAY UNTUK SISTEM KEAMANAN DESAIN DAN IMPLEMENTASI *NETWORKING SECURITY* MEMANFAATKAN *SECURITY CONFIGURATION WIZARD (SCW)*

Supratman Zakir
Program Studi Pendidikan Teknik dan Komputer Informatika, Fakultas Tarbiyah dan Ilmu Keguruan
IAIN Bukittinggi
Jl. Raya Gurun Aur Kubang Putih Bukittinggi
e-mail : supratman@iainbukittinggi.ac.id

ABSTRAK

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek yang penting dari suatu sistem informasi. Sistem operasi Microsoft Windows Server 2008 memberikan fasilitas baru yang berkaitan dengan aspek keamanan yaitu Windows Firewall with Advanced Security yang merupakan fasilitas dari Security Configuration Wizard. Dengan fasilitas tersebut memungkinkan pengguna untuk membuat policy atau rules yang sesuai dengan kebutuhan. Dalam penelitian ini, dibahas tentang bagaimana membangun keamanan jaringan dengan memanfaatkan Windows Firewall with Advanced Security. Dalam implementasinya, peneliti membuat rancangan dengan sebuah server menggunakan sistem operasi Windows Server 2008 dan sebuah client dengan sistem operasi Windows Vista Ultimate. Rule-rule yang berkaitan dengan keamanan dibuat, baik di server,maupun di client. Rancangan sistem kemanan yang dibuat, berdasarkan referensi-referensi yang relevan dengan penelitian, begitu juga dengan rule-rule yang akan diterapkan. Setelah rule-rule tersebut dibuat, lalu dilakukan pengujian terhadap rule-rule tersebut. Dari hasil pengujian terungkap bahwa fasilitas Windows Firewall with Advanced Security yang merupakan fasilitas dari Security Configuration Wizard pada sistem operasi Microsoft Windows Server 2008 mampu menawarkan sistem keamanan yang baik terhadap serangan, baik serangan yang datang dari luar maupun dari dalam sistem jaringan sendiri.

Kata kunci : Firewall, Security, Security Configuration Wizard, Windows Firewall

ABSTRACT

The security problem and data privacy are one of the most important aspect from information system. The operation system of Microsoft Windows Server 2008 gives some new facilities; including thing that relates to the security aspect is Windows Firewall with Advanced Security. With that facilities enable the user to make individual rules that suitable with the security need of network. In this observation it is discussed about how to develop the network of security with the use of Windows Firewall with Advanced Security which is mainly discussed about how to make the rules that relate with firewall. In the implementation the writer makes a plan with a server using operation system of Windows Server 2008 and also computer client. The plan of security system that is made based on many references that relate with observation and also with the rules are applied after the rules are made, than do some observation about the rules. From the result of observation pronounced actually Windows Firewall with Advanced Security facilities in the Operation System of Microsoft Windows Server 2008 able to offer the good security system about attack, that attack come from outside oven though the attack from the network system it self.

Keyword : *Firewall, Security, Security Configuration Wizard, Windows Firewall*

1. PENDAHULUAN

Perkembangan teknologi informasi merupakan salah satu bentuk usaha untuk mengelola informasi supaya dapat berdaya guna bagi organisasi. Perkembangan teknologi komputer dan jaringan (Internet) menjadi bukti begitu pentingnya pengorganisasian informasi. Pentingnya pengelolaan informasi yang

profesioanal dan proporsonal terkait dengan persaingan baik secara lokal, regional maupun global. Sehingga, diperlukan sebuah sistem pengelolaan informasi yang saat ini telah banyak diimplementasikan dalam berbagai bidang seperti, Sistem Informasi Akuntansi (SIA), Sistem Informasi Manajemen (SIM), Sistem Informasi Produksi (SIP), Sistem Informasi Sumber Daya Manusia.

Sejalan dengan perkembangan sebuah organisasi, cara penyampaian informasipun bekembang sesuai dengan perkembangan teknologi informasi. Transaksi yang sering berlangsung di tempat yang berbeda, kebutuhan informasi yang cepat untuk mengambil keputusan, keberadaan kantor-kantor cabang sebuah organisasi, prinsip kemitraan dan gangguan keamanan jika data atau informasi dikirim dalam bentuk fisik, menjadikan teknologi informasi terutama teknologi jaringan sebagai solusi jitu dan cerdas untuk diimplementasikan dalam sebuah organisasi. Perkembangan teknologi jaringan juga tidak kalah pesatnya dengan teknologi-teknologi lain dalam dunia teknologi informasi, pergeseran paradigma teknologi jaringan sistem *wire* (kabel) ke teknologi nirkabel (*wireless)* menarik bagi para pengambil kebijakan organisasi untuk menggunakan teknologi tersebut. Transformasi ini memberikan solusi pada dua masalah keamanan data, yaitu masalah privasi (*privacy*) dan keautentikan (*authentication*). Privasi mengandung arti bahwa data yang dikirimkan hanya dapat dimengerti informasinya oleh penerima yang sah. Sedangkan keautentikan mencegah pihak ketiga untuk mengirimkan data yang salah atau mengubah data yang dikirimkan.

Ancaman dapat dilakukan seseorang atau proses yang mengeksploitasi suatu keadaan yang rentan atau lemah dalam bidang keamanan yang biasa disebut dengan *vulnerability*. Beberapa keadaan yang dikategorikan *vulnerability* adalah lemahnya otentikasi dan otorisasi serta implementasi keamanan yang lemah. Ancaman terhadap keamanan terbagi atas dua kategori umum, yaitu ancaman pasif dan ancaman aktif. Ancaman pasif disebut juga dengan mendengarkan secara diam-diam *(Eavesdropping)*, mencakup upaya-upaya penyerang *(hacker* dan *intruder)* mendapatkan informasi yang berkaitan dengan suatu komunikasi. Sedangkan ancaman aktif mencakup beberapa modifikasi data yang ditransmisikan atau mencoba membuat sebuah data yang sedang ditransmisikan tidak sampai pada tujuan yang dituju. Ancaman atau serangan lewat jaringan adalah serangan yang memanfaatkan koneksi antar komputer sebagai media utamanya. Biasanya penyerang mengumpulkan data sistem saat korbannya terhubung ke jaringan. Metode lain adalah menanam program kecil ke dalam sistem jika korban tidak intensif menggunakan jaringan, dan akan aktif saat jalur jaringan dibuka. Beberapa jenis serangan pada sistem komputer maupun jaringan, yaitu *virus, spyware, worm, root kit, spam, phishing, DoS (denial of service), Sniffer, Spoofing*, *Man-In-The-Middle Attack* dan *Trojan Horse*.

Virus merupakan penggalan kode yang dapat menggandakan dirinya sendiri dengan cara menyalin kode dan menempelkan ke berkas program yang dapat dieksekusi. Selanjutnya salinan virus ini akan menjadi aktif manakala program yang terinfeksi dijalankan. *Spyware* memiliki tingkat bahaya yang jauh lebih rendah dibanding *virus*, akan tetapi *spyware* tetap harus diwaspadai. Pasalnya serangan ini bisa mencuri data penting di sebuah PC tanpa disadari korbannya. Jalur *internet* adalah media utama untuk menanam *spyware*. *Worm* merupakan program yang dapat menggandakan dirinya sendiri dan menulari komputer yang terhubung dalam jaringan. Berbeda dengan *virus, worm* merupakan sebuah program komputer kecil yang bisa menyebar tanpa harus menumpang pada file tertentu (otonom). *Root Kit* sebenarnya bukan sebuah program yang berbahaya, karena diciptakan untuk melindungi hak paten bagi produk hiburan digital seperti CD *Audio* dan *DVD*. Hanya saja seiring berjalannya waktu, *Root Kit* disalahgunakan pihak tertentu untuk meraup keuntungan. *Root Kit* yang sudah dimodifikasi bisa masuk ke dalam sistem operasi dengan hak akses *administrator*. Akibatnya, pemilik *Root Kit* memiliki kontrol penuh terhadap PC korbannya. Bahayanya lagi, *Root Kit* pandai menyembunyikan diri dan menyamar sebagai modul, *driver* atau bagian lain dari sistem operasi, sehingga tidak mudah untuk menemukannya. *Spam* sebenarnya tidak berbahaya, selama tidak ditumpangi oleh virus, *root kit* atau *file* berbahaya lain. Serangan yang datang lewat email ini biasanya digunakan untuk sarana penawaran produk atau jasa. Hanya saja jika terlampau banyak, maka jaringan akan menjadi sibuk oleh lalu-lintas *email* yang tidak jelas peruntukkannya. *Phishing* sebenarnya lebih cocok dimasukkan ke dalam kategori penipuan. Ini karena *phishing* sangat mudah dibuat, tetapi memiliki akibat kerugian yang cukup besar. Untuk membuat *phising*, tidak harus memiliki keahlian menjebol sistem yang canggih. Cukup memahami apa yang disebut *social engineering atau pengelabuan (mengelabui orang lain)*, atau kelemahan orang saat mengintepretasikan sebuah informasi di komputer. *DoS (denial of service)* metode serangan *DoS* digunakan untuk membuat sebuah *host* menjadi *overload* dengan membuat begitu banyak permintaan di mana *reguler traffic* diperlambat atau kadang-kadang diinterupsi. Serangan *DoS* tidak sampai memasuki sebuah target, karena sasaran penyerang hanyalah membuat target menjadi *overload* dengan begitu banyak *traffic* palsu yang tidak dapat diatasi. *Sniffer, t*eknik ini diimplementasikan dengan membuat program yang dapat melacak paket data seseorang ketika paket tersebut melintasi jaringan, menangkap

password atau menangkap isinya. *Spoofing* melakukan pemalsuan alamat *e-mail* atau *web* dengan tujuan untuk menjebak pemakai agar memasukkan informasi yang penting seperti *password.* Serangan ini mengeksploitasi hubungan dengan mengizinkan penyerang untuk mengasumsikan identitas *host* yang dipercaya. *Man-In-The-Middle* merupakan serangan dengan cara "mendengarkan" data yang lewat saat 2 (dua) terminal sedang melakukan komunikasi dan kedua terminal tersebut tidak dapat mengetahui adanya pihak ketiga di tengah jalur komunikasi mereka. *Trojan Horse* merupakan program yang dirancang agar dapat digunakan untuk menyusup ke dalam sistem komputer tanpa sepengetahuan pemilik komputer. *Trojan horse* ini kemudian dapat diaktifkan dan dikendalikan dari jarak jauh atau dengan menggunakan *timer* (waktu). Akibatnya, komputer yang disisipi *trojan horse* dapat dikendalikan dari jarak jauh

Beberapa cara yang dapat digunakan untuk menangkal berbagai bentuk serangan seperti di atas adalah privasi (*privacy*) dan keotentikan (*authentication*). Privasi mengandung arti bahwa data yang dikirimkan hanya dapat dimengerti informasinya oleh penerima yang sah. Sedangkan keotentikan mencegah pihak ketiga untuk mengirimkan data yang salah atau mengubah data yang dikirimkan.

Keamanan dan kerahasiaan pada jaringan komputer saat ini menjadi isu yang terus berkembang. Perusahaan *Software* seperti *Microsoft* meluncurkan beberapa sistem operasi jaringan (*Network Operating System)* yang didesain untuk mengidentifikasi kebutuhan fungsional dari sebuah server. Salah satu kebutuhan fungsional tersebut adalah keamanan (*security).* Beberapa produk *Microsoft* untuk sistem operasi jaringan adalah *Windows NT, Windwows Server 2000, Windows Server 2003* dan yang terakhir adalah *Windwos Server 2008.* Sistem operasi jaringan yang dikeluarkan *Microsoft* yaitu *Microsof Windows Server 2003* telah banyak digunakan oleh bebagai kalangan, bisnis, pendidikan, penelitian dan lain sebagainya. Hal ini dikarenakan sistem tersebut memiliki fitur-fitur yang mampu mengelola jaringan dengan baik salah satunya adalah kemampuan membuat *firewall* sebagai keamanan atau penangkal dari penyusup maupun para *hacker.* Akan tetapi seiring dengan perkembangan teknologi informasi, teknologi yang digunakan para *Intruder* maupun para *hacker* juga semakin tinggi, untuk mengantisipasi hal tersebut *Microsoft* mengeluarkan sistem operasi jaringan baru yaitu *Microsoft Windows Server 2008* yang memiliki fungsionalitas lebih baik dari pendahulunya. *Advanced Security* merupakan salah satu fitur pada *Windows Server 2008* yang untuk meningkatkan keamanan setiap komputer dengan cara memblok *network traffic* yang tidak diinginkan yang akan memasuki komputer tersebut.

Berdasarkan latar belakang masalah yang telah diuraikan di atas, maka dapat dirumuskan permasalahan penelitian sebagai berikut :

1. Bagaimana membangun sistem keamanan jaringan yang mapan pada *Hotspot* STAIN Bukittinggi ?
2. Bagaimana membangun sistem keamanan jaringan yang mapan tanpa menganggu atau menurunkan performa jaringan secara keseluruhan ?
3. Bagaimana membangun sistem keamanan jaringan yang mapan tanpa menambah beban biaya yang lebih tinggi ?
4. Bagaimana *Windows Firewall* menerapkan *rule-rule* dalam pengamanan sistem ?
5. Bagaimana Sistem Operasi *Windows Server 2008* menerapkan *policy* untuk *Security Configuration Wizard ?*
6. Bagaimana sistem kerja *Security Configuration Wizard* pada sistem operasi *Windows Server 2008* ?

Dalam penelitian ini, penulis membatasi pembahasan penelitian sebagai berikut :

1. Penelitian dilakukan pada Jaringan *Hotspot* STAIN Bukittinggi
2. Keamanan jaringan yang akan dibangun memanfaatkan *Security Configuration Wizard* pada Sistem Operasi Windows Server 2008.
3. Mengkaji sistem kerja *Security Configuration Wizard* pada sistem operasi *Windows Server 2008*
4. Menganalisis penerapan *policy* untuk *Security Configuration Wizard* pada Sistem Operasi *Windows Server 2008*.
5. Menganalisis bagaimana *Windows Firewall* pada *Windows Server 2008* membangun *rule-rule* dalam rangka pengamanan sistem

Sementara tujun dari penelitian ini adalah untuk :

1. Membangun sebuah sistem keamanan jaringan pada jaringan *Hotspot* STAIN Bukittinggi dengan memanfaatkan *Security Configuration Wizard* pada Sistem Operasi *Windows Server 2008* tanpa mengurangi performa kerja jaringan.
2. Mengkaji sistem kerja *Security Configuration Wizard* pada sistem operasi *Windows Server 2008*

3. Menganalisis penerapan *policy* untuk *Security Configuration Wizard* pada Sistem Operasi *Windows Server 2008*.
4. Menganalisis bagaimana *Windows Firewall* pada *Windows Server 2008* membangun rule-rule dalam rangka pengamanan sistem.

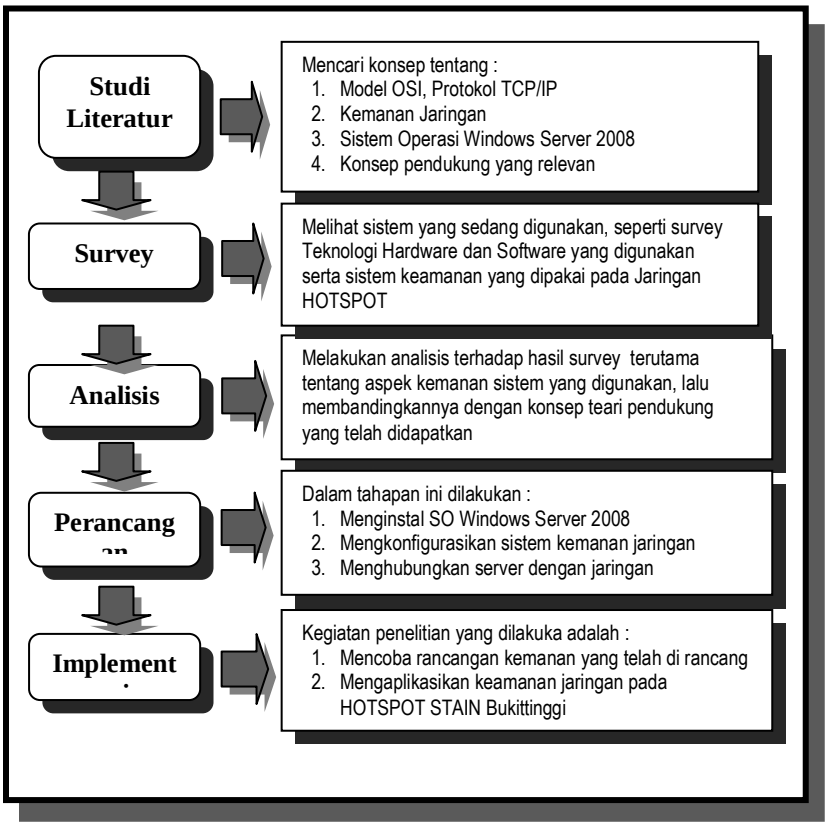
2. METODE PENELITIAN

2.1. Tempat Penelitian

Tempat penelitian ini dilaksanakan di Sekolah Tinggi Agama Islam Negeri (STAIN) Bukittinggi. Pemilihan tempat penelitian didasarkan atas pertimbangan bahwa kondisi dan sarana (objek) yang diteliti sudah dianggap layak untuk dilakukannya penelitian.

2.2. Tahapan Penelitian

Dalam melaksanakan penelitian peneliti mengikuti beberapa proses atau tahapan sebagai berikut :



Gambar 1. Tahapan Penelitian

Adapun lebih jelasnya kegiatan-kegiatan yang dilakukan dalam tahapan penetian adalah sebagai berikut:

1. Studi Literatur

Dalam tahapan ini peneliti mengadakan studi untuk mencari teori dan konsep yang berhubungan dengan penelitian. Studi literatur ini dilakukan baik melalui talaah buku atau jurnal-jurnal di perpustakaan maupun mencari sumber-sumber dari *internet.* Teori atau konsep yang di telaah adalah yang berkaitan dengan objek dan permasalahan penelitian, yaitu Model OSI *(Open System Interconnection)*, Protocol TCP/IP, Keamanan jaringan, Aspek/service keamanan, Serangan pada Jaringan Komputer, Tinjauan Keamanan Jaringan, DES (*Data Encryption Standard), Firewall*, Evaluasi Sistem Keamanan Jaringan, Mengamankan Sistem Jaringan, *Overview* Sistem Operasi *Windows Server 2008*, Protokol pada *Windows Server 2008*, *Group Policy Object, Security Configuration Wizard (SCW), Windows Firewall with Advanced Security, Host Firewall* serta konsep-konsep yang mendukung penelitian ini.

2. Survey

Survey dilakukan untuk melihat sistem yang sedang berjalan, terutama tentang sistem keamanan yang diterapkan. Adapun beberapa aspek yang disurvey adalah teknologi hardware yang digunakan meliputi; komputer *server* dan komputer *clien;* teknologi jaringan yang digunakan yang meliputi; *Switch* dan *Access Point.* Selanjutnya *software* yang digunakan seperti Sistem operasi pada komputer *server* dan pada *client* serta bentuk keamanan jaringan yang dipakai pada sistem saat ini.

3. Analisis

Pada tahapan ini peneliti melakukan analisis dan evaluasi terhadap sistem yang sedang berjalan, dimana hasil analisis digunakan untuk proses desain keamanan jaringan. Beberapa aspek yang dianalisis pada objek penelitian, peneliti kelompokkan menjadi 3 (tiga) bagian utama, yaitu pertama; *Human* yang meliputi orang-orang yang terlibat dalam operasional sistem jaringan *Hotspot* STAIN Bukittinggi, kedua; aspek *object* meliputi sistem kerja *Hotspot* dan ketiga adalah aspek teknologi yang meliputi semua sistem teknologi yang mendukung jalannya sistem *Hotspot* STAIN Bukittinggi. Tujuan utama menganalisis semua aspek di atas adalah untuk mengidentifikasi permasalahan sistem, mencari beberapa alternatif solusi terhadap masalah sistem yang ditemukan, memilih dan mempertimbang solusi alternatif yang telah ditentukan serta membuat rancangan secara logik solusi yang dipilih. Hasil dari analisis secara keseluruhan didokumentasikan lalu akan ditinjau lagi dengan memperbandingkannya dengan konsep-konsep atau teori-teori tentang permasalahan penelitian.

4. Perancangan

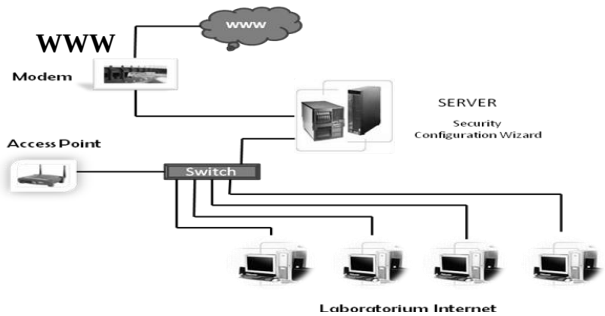
Tahapan ini merupakan tahapan yang berupa penggambaran, perencanaan dan pembuatan sketsa atau pengaturan dari beberapa elemen yang terpisah ke dalam satu kesatuan yang utuh dan berfungsi, termasuk menyangkut mengkonfigurasikan dari komponen-komponen perangkat lunak dan perangkat keras dari suatu sistem. Beberapa kegiatan yang peneliti lakukan adalah, mengkonfigurasikan komputer yang akan dijadikan *server* dan *client*. Menginstall sistem operasi *Windows Server 2008* pada komputer *server* dan menginstal sistem operasi *Windows XP SP2* pada komputer *client*.

5. Implementasi

Implementasi merupakan tahapan dalam membanguan sebuah sistem keamanan jaringan berdasarkan hasil analisis data, yang akan menjawab permasalahan penelitian. Adapun beberapa kegiatan dalam tahapan ini meliputi mengkonfigurasi Sistem Operasi *Windows Server 2008* yang telah dipasang pada komputer *server* dan mengkonfigurasi *rule-rule* atau seting keamanan jaringan yang akan disimpan ke dalam *group policy object* (GPO) kemudian akan diterapkan untuk dipatuji oleh user dalam jaringan. Setelah semua *rule* dikonfigurasin, sistem akan diuji dengan sebuah *software* dalam hal ini peneliti akan menggunakan software *Winuke* yang bertujuan untuk melihat ketahanan atau tingkat keamanan sistem yang telah dibangun.

2.3. Desain Penelitian

Adapun desain penelitian dapat digambarkan sebagai berikut :



SWITCH Gambar 2. Desain sistem penelitian

2.4. Implementasi Desain Penelitian

Beberapa kegiatan implementasi diantaranya pemilihan perangkat keras *(Hardware)* seperti *server*, *client* dan perangkat jaringan. Setelah perangkat keras dipasang, dilanjutkan dengan instalasi perangkat lunak *(Software)*. Beberapa kegiatan pada tahap ini adalah instalasi Sistem Operasi (SO)

Windows Server 2008 pada *server*, instalasi *Windows Vista Ultimate* pada *client.* Langkah selanjutnya adalah memeriksa *Default Setting*, baik pada *server* maupun pada c*lient*. selanjutnya secara berurutan adalah membuat *Rule* yang meng-*Allow Inbound Network Traffic*, dan mem-*Block Outbound Network Traffic*, dilanjutkan dengan menerapkan *Basic Domain Isolation Policy*, *m*engisolasi Server, membuat *Security Group*, dan memodifikasi *Firewall Rule* untuk *Require Group Membership and Encryption.*

3. PEMBAHASAN

Setalah hasil desain dimplementasikan, maka dilakukan pengujian terhadap desain tersebut. Beberapa kegiatan dalam tahap ini adalah sebagai berikut; menguji *Inbound Rule* untuk mem-*allow network traffic*, menguji *Rule* untuk spesifik komputer yang di-*allow inbound traffic*, menguji *Outbound Rule* untuk mem-*block network traffic*, dan menguji *Rule* ketika *User1* bukan *member group.*

3.1. Hasil Pengujian

Hasil imlementasi pemeriksaan terhadap *setting default Firewall* yang dilakukan melalui pemeriksaan melalui *Control Panel*, terlihat bahwa secara *default*, *Firewall* otomatis aktif pada sistem operasi yang terpasang, terlihat bahwa *Windows Firewall is on*, hal tersebut manyatakan bahwa jika *Firewall* aktif, maka *inbound connection* yang tidak termasuk dieksepsi (diterima) akan diblok oleh *windows firewall.* Hasil implementasi pembuatan *rule* untuk meng-*allow Inbound Network Traffic Rule* yang dibuat sespesifik mungkin. Itu artinya harus menspesifikasikan program dan *port*, untuk memastikan hanya program dan *port* tertentu saja yang dapat menerima *traffic.* Secara *default*, *windows firewall* meng-*allow* semua *outbound network traffic*. Jika institusi atau organisasi menginginkan untuk melarang keluarnya informasi atau sebuah program, maka dapat dibuat *rule* agar program tersebut tidak dapat melakukan koneksi. Pada tahap implementasi, pembuatan *rule* untuk mem-*block outbound nework traffic* dilakukan dengan menggunakan fasilitas *Group Policy Management* yang ada pada *windows server 2008.*

Sementara itu, penerapan *Domain Policy* pada *domain isolation*, dimaksudkan untuk otentikasi agar setiap komputer yang berhubungan dalam koneksi dapat memastikan identitas komputer lainnya. Dengan membuat *rules* yang mengharuskan otentikasi oleh *domain member*, maka secara efektif dapat mengisolasi komputer *domain-member* tersebut dari komputer yang bukan bagian dari *domain*. Hasil penerapan *Domain Policy* dengan membuat *rule* maka akan dapat dibuat seluruh *member computers require authentication* untuk meng-*inbound network traffic*, dan *request authentication* untuk meng-*outbound traffic*. Pembuatan *rule* dilakukan melalu fasilitas *Group Policy Management* seperti yang telah dibahas pada bab sebelumnya.

Pengisolasian *server* dimaksudkan untuk membatasi *domain-member computer* yang akan berkomunikasi hanya dengan *domain-member computer* yang diberi izin. Hal ini dilakukan karena beberapa *server* memiliki data yang sensitif seperti, *personal data*, *medical records*, atau *credit card data* yang harus dijaga dengan lebih hati-hati. Membatasi akses ke sensitif data tersebut hanya kepada *user* yang memiliki kepentingan yang spesifik.

Dengan menggunakan *Windows Firewall with Advanced Security in Windows Server 2008*, dapat dipesifikasikan bahwa spesifik *network connection* hanya dapat diakses oleh suatu *user*, berdasarkan *group membership*-nya. Disamping itu juga dapat dispesifikasikan bahwa akses dibolehkan hanya bagi suatu komputer berdasarkan *computer account membership* dalam suatu *group*.

3.2. Analisis Hasil Penelitian

Dari hasil pengujian terhadap *rules* yang telah dibuat untuk memblok *network traffic*, terlihat bahwa ketika salah satu *service* dalam penelitian ini penulis menggunakan service *telnet*, maka eksekusi tersebut akan akan gagal dan mengeluarkan pesan *time out*, hal ini disebabkan oleh karena *firewall di server* sekarang memblok seluruh *inbound traffic ke Telnet service.*

Rule di atas dapat dirubah supaya service *telnet* dapat dieksekusi, ketika *rule* dirubah maka eksekusi akan sukses dilaksanakan karena *firewall* meng-*allow inbound traffic* ke *Telnet service port 23.*

Hasil pengujian terhadap *Outbound Rule* untuk meng-*allow network traffic*, terlihat koneksi gagal dan menampilkan pesan *error* sebagai berikut: *Connecting to server…Could not open connection to the host, on port 23: Connect failed*

Jika ingin mengizinkan trafik keluar dari jaringan, maka *rule* yang telah dibuat dapat dinonaktifkan. Dari hasil pengujian terlihat koneksi *telnet* akan tersambung ke *port 23*, karena *rule Block Oubound* sudah dinonaktifkan.

Sementara hasil pengujian setelah *rule* dikonfigurasikan, maka koneksi computer *client* (*user1)* akan berhasil, karena komputer *client (user1)* telah ditambahkan ke dalam *computer group* yang

direferensikan di *inbound Telnet firewall rule* untuk *server*. Akan tetapi jika *rule* tidak dibuat maka komunikasi agan mengalami kegagalan, sebab computer *server* membutuhkan *group membership* ataupun *encryption* untuk *Event Viewer*

4. KESIMPULAN

Uraian dan pembahasan sebelumnya maka dapat diambil kesimpulan bahwa *Windows Firewall with Advanced Security* yang merupakan fasilitas dari *Security Configuration Wizard* adalah elemen yang penting dalam *defense-in-depth security strategy* untuk membantu anda mengamankan komputer dalam suatu organisasi, dan membantu dalam mitigasi melawan ancaman yang mem-*bypass* parameter *firewall* atau yang berasal dari dalam *network* itu sendiri.

Seperti yang telah dibahas sebelumnya, bahwa *Windows Firewall with Advanced Security* mengkombinasikan *host-based firewall* dan *Internet Engineering Task Force (IETF)*- yang merupakan implementasi dari *Internet Protocol security (IPsec)*. Sebagai sebuah *host-based firewall*, *Windows Firewall with Advanced Security* berjalan pada setiap komputer yang menjalankan Windows Server® 2008 untuk memberikan proteksi dari serangan pada jaringan yang mungkin dapat melewati perimeter *netwok firewall*, ataupun serangan yang berasal dari dalam organisasi.

Windows Firewall with Advanced Security juga menyediakan *computer-to-computer connection security* berbasis *IPsec* yang membantu melindungi *network data* dengan cara mengeset *rules* sehingga dibutuhkan otektikasi, *integrity checking*, ataupun enkripsi ketika komputer-komputer di dalam suatu organisasi bertukar data.

Beberapa fitur yang dibawa oleh *Windows Firewall with Advanced Security* diantaranya :

1. *Windows Firewall with Advanced Security* yang merupakan fasilitas pada *Security Configuration Wizard* menyediakan fasilitas untuk *set up basic inbound* dan *outbound firewall rules*
2. Dengan *Windows Firewall with Advanced Security* dapat membuat *Group Policy object* yang mengkonfigurasi *firewall setting* di setiap komputer dalam suatu domain, dan memastikan bahwa user tidak dapat mengganti setting tersebut.
3. Dengan *Windows Firewall with Advanced Security* dapat dibuat satu *set basic domain isolation rules* yang membatasi *domain-member* komputer agar tidak menerima koneksi dari komputer yang bukan member dari domain.
4. Dengan *Windows Firewall with Advanced Security* dapat dibuat *connection security rules* yang mengisolasi *server* penting, tempat informasi sensitif, dengan membatasi akses hanya kepada komputer yang menjadi member dari group yang disetujui.
5. Dengan *Windows Firewall with Advanced Security* dapat dibuat *rule* yang secara spesifik menentukan komputer mana yang dapat mem-*bypass firewall*.

Dengan fasilitas-fasilitas baru tersebut *Windows Firewall with Advanced Security* pada sistem operasi *Windows Server 2008* terbukti mampu memberikan sistem keamanan yang baik terhadap serangan baik yang datang dari luar maupun dari dalam.

Dari penelitian yang telah dilakukan serta berdasarkan referensi yang relevan, maka terdapat beberapa hal penting yang dapat dijadikan bahan sebagai saran baik untuk melakukan penelitian ataupun untuk pengembangan yang lebih lanjut yang tentunya harus lebih baik dari penelitian yang sudah ada ini. Adapun di anaranya adalah :

1. Dalam penerapan suatu keamanan jaringan dalam hal ini adalah teknologi *firewall*, perlu pertimbangan kemajuan dunia teknologi informasi saat ini, karena saat ini telah banyak produk-produk ataupun varian-varian *firewall*. Karena itu ada baiknya mempertimbangkan *firewall* yang cocok dan sesuai dengan kebutuhan organisasi.
2. Pemilihan sistem operasi *Windows Server 2008*, karena ini merupakan system operasi *server* terbaru yang dilekuarkan oleh *Microsoft*, hal ini membuat penulis sangat kekurangan dengan referensi-referensi yang relevan dengan pembahsan penelitian yang berakibat dengan kedangkalan pembahasan. Dari itu peneliti berhaharp ada penelitian lanjutan dengan tema pembahasan mengenai keamanan jaringan dengan *Windows Server 2008.*
3. Dalam melaksanakan implementasi peneliti sarankan untuk lebih memperluas jaringan seperti untuk jaringan internet, serta dapat menggunakan *software* khusus dalam pengujian sistem yang telah dirancang, sehingga system keamanan yang dirancang benar-benar teruji untuk menjadi *firewall* dalam sebuah sistem jaringan

DAFTAR PUSTAKA

[1] Abdul Kadir, (2003), *Pengenalan Sistem Informasi*, Yogjakarta, Andi Offset.

[2] Angga Danimartiawan, dkk, (2002), *IPsec: Aplikasi Teknik Kriptografi untuk Keamanan Jaringan Komputer*, makalah tidak diterbitkan

[3] Budi Rahardjo (2002), *Keamanan Sistem Informasi Berbasis Internet*, Bandung PT. Insan Infonesia, Jakarta, PT. INDOCISC.

[4] Harianto Ruslim (2005), *Hack Attack : Konsep, Penerapan dan Pencegahan*, Jasakom, cet. I

[5] Onno W. Purbo, dkk, (2002), *Buku Pintar Internet TCP/IP Standar, Desain dan Implementasi*, Jakarta, PT. Elex Media Komputindo

[6] S'To (2006), *Seni Internet Hacking ReCODED*, Jasakom

[7] ----------(2006), *Computer Worm 1 - Secret of Underground Coding*, Jasakom

[8] ---------- (2004), *Mengenal Windows 2003*, Jakarta, PT. Elex Media Komputindo

[9] Stalling, William (2002), *Data & Computer Communication*, diterjemahkan oleh Thamir Abdul Hafedh Al-Hamdany, Jakarta, Salemba Teknika, Edisi I

[10] Thomas, Tom (2004), *Network Security First Step*, terjemahan oleh Tim Penerjemah ANDI offset, Yogyakarta, Andi Offset.

[11] Dikshie Fauzi (2002), *Tinjauan Mekanisme dan Aplikasi Ipsec: Studi Kasus VPN*, Makalah tidak diterbitkan.

[12] Ferguson, N., and Schneier, B., (2000) *A Cryptographic Evaluation of IPSec*, *Counterpane Internet Security*, Makalah tidak diterbitkan Didik Dwi Prasetyo (2004), *Mail Server Berbasis Java pada Server Windows dan Linux*, Jakarta, PT. Elex Media KomputindoAdnan Basalamah, (1999), *Internet & Email Security*, Makalah online tidak diterbitkan www.bogor.net/idkf/idkf/network/network-security/ppt-internet-and-email-security-10-1999.ppt

[13] Fajar Faturrahman (2008), *Pengenalan Windows Server 2008*, Windows Server Sistem, http://wss-id.org/blogs/fajar/archive/2007/10/21/pengenalan-windows-server-2008.aspx

[14] Jethefer, Stevens, (2007), *Studi dan Perbandingan Algoritma IDEA (International Data Encryption Algorithm) Dengan DES (Data Encryption Standard)*, Makalah tidak diterbitkan, http://www.informatika.org/~rinaldi/Kriptografi/2006-2007/Makalah1/Makalah1-005.pdf

[15] Narenda Wicaksono (2008), *Windows Server 2008 : Langkah Demi Langkah Panduan Konfigurasi Two-Node Print Server Failover Cluster*, Microsft Innovation Center Institut Teknologi Bandung, http://wss-id.org/files/narenda

[16] ---------- (2008), *Windows Server 2008 : Panduan Langkah demi Langkah Penerapan Policy untuk Windows Firewall with Advanced Security*, Microsft Innovation Center Institut Teknologi Bandung, http://wss-id.org/files/narenda

[17] ---------- (2008), *Windows Server 2008 : Windows Server Active Directory Rights Management Services Step-by-Step Guide*, Microsft Innovation Center Institut Teknologi Bandung, http://wss-id.org/files/narenda

[18] ---------- (2008), *Windows Server 2008 : Panduan Langkah demi Langkah: Menerapkan SSTP Remote Access*, Microsft Innovation Center Institut Teknologi Bandung, http://wss-id.org/files/narenda

[19] ---------- (2008), *Windows Server 2008: Panduan Setup Lisensi TS Windows Server 2008*, Microsft Innovation Center Institut Teknologi Bandung, http://wss-id.org/files/narenda

[20] ---------- (2008), *Windows Server 2008: Changes in Functionality from Windows Server 2003 with SP1 to Windows Server 2008*, Microsft Innovation Center Institut Teknologi Bandung, http://wss-id.org/files/narenda

[21] Nita Rahmi, (2008), *Studi dan Analisis Penggunaan Key-Schedule pada Algoritma IDEA* (*International Data Encryption Algorithm*), Makalah tidak diterbitkan, http://www.informatika.org/~rinaldi/Kriptografi/2006-2007/Makalah1/Makalah1-005.pdf

[22] Tutang (2008), *Windows Server 2008 : Panduan Langkah-Langkah Opsi Instalasi Server Core pada Windows Server 2008*, Microsft Innovation Center Institut Teknologi Bandung, http://wss-id.org/files/tutang.