ISSN: 2302-3805

Perancangan dan Pengembangan Keamanan Jaringan *Enterprise* dengan VPN

A. Donny Mahendra [1] , Ema Utami [2] , Abas Ali Pangera [3]

[1] Mahasiswa Magister Teknik Informatika Program Pascasarjana STMIK AMIKOM Yogyakarta
[2] Dosen Magister Teknik Informatika Program Pascasarjana STMIK AMIKOM Yogyakarta
[3] Dosen Program Studi Teknik Informatika STMIK AMIKOM Yogyakarta
Jl. Ring Road Utara Condong Catur Depok Sleman Yogyakarta
email : donny@gioia.web.id [1], ema.u@amikom.ac.id [2] , abas@amikom.ac.id [3]

Abstrak

PT. Time Excelindo adalah sebuah perusahaan penyedia teknologi informasi yang mempunyai cabang dan mobilitas karyawan yang cukup tinggi. Menuntut jaminan keamanan yang prima dalam setiap transaksi yang dilakukan, karena menurut survey pada tahun 2011 oleh Verizon dan Computer Security Institute (CSI) ditemukan masih adanya ancaman keamanan dari internal oleh intruder. Penelitian ini menggunakan OpenVPN sebagai aplikasi inti sistem keamanan VPN yang dibangun, dengan beberapa pengembangan kebijakan dalam aspek teknis dan non-teknis. NIST 800-115 digunakan untuk menguji sistem dan ISO 27002:2005 digunakan untuk penyusunan kebijakan yang terkait, untuk evaluasi teknis menggunakan Proof-of-Concept dan audit internal untuk evaluasi kebijakan. Hasil penelitian menunjukkan bahwa OpenVPN dapat secara teknis mengikuti kebijakan-kebijakan yang dibuat.

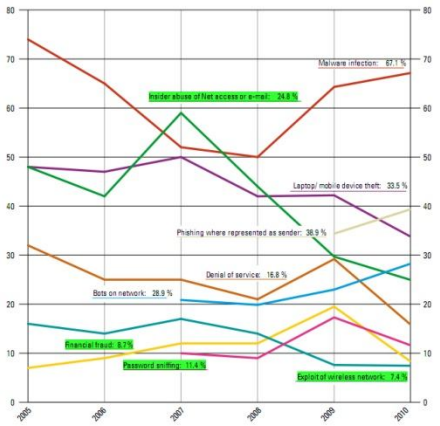
Kata Kunci : *vpn, nist 800-115, iso 27002:2005, insider*

1. Pendahuluan

Jaringan komputer yang terintegrasi saat ini sudah menjadi kebutuhan utama bagi sebuah institusi atau perusahaan bisnis, khususnya pada PT. Time Excelindo (TE) yang memiliki cabang di lokasi geografis yang berbeda dan juga perusahaan yang mana karyawan tidak hanya bekerja di dalam kantor saja, tetapi juga *mobile. Mobile* saat ini tidak hanya diartikan bekerja di luar area kantor, tapi juga diartikan bekerja dalam satu area kantor dengan berpindah ruangan. Oleh karena itu diperlukan kemudahan untuk dapat mengakses sumber daya yang ada di kantor pada saat diperlukan dimanapun dan kapanpun karyawan tersebut berada.

Perusahaan tentunya memiliki sistem penunjang operasional berbasis Teknologi Informasi (TI) seperti Network Management System (NMS), Customer Relationship Management (CRM), Document Management System (DMS), Email, Internet Banking dan aplikasi Enterprise lainnya. Di era teknologi informasi sekarang ini bukan merupakan suatu hal yang sulit untuk melakukan proses komunikasi data, cukup terhubung dengan jaringan komputer, proses pertukaran informasi dapat dilakukan. Namun ada beberapa hal yang harus diperhatikan dalam proses tersebut, diantaranya: Teknologi, Arsitektur, Skalabilitas, serta Keamanan.

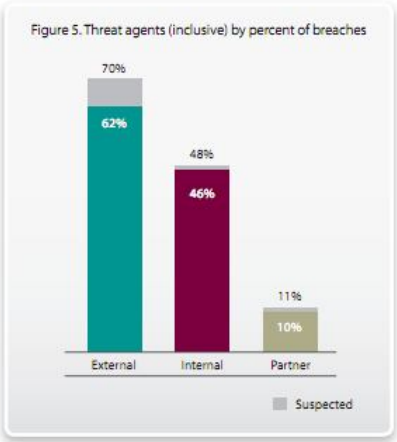
Jaringan komputer merupakan tulang punggung dalam proses pertukaran informasi baik itu di lingkungan internal ataupun external perusahaan yang pada dasarnya tidaklah aman, terlebih apabila jaringan tersebut terkoneksi dengan internet.



Gambar 1 Kategori serangan insider (CSI,2010)

Menurut survei yang dilakukan CSI (Richardson, 2010) seperti yang tertuang dalam Gambar 1 dapat diketahui bahwa serangan atau gangguan dari dalam *(insider)* masih cukup besar. Serangan tidaklah selalu berasal dari luar, dari dalam pun sangat dapat dimungkinkan terjadinya penyadapan dan hacking pada jaringan internal. Pada Gambar 2, dapat terlihat bahwa hal ini diperkuat dengan penelitian yang dilakukan oleh Verizon *Response-Intelligence-Solutions-Knowledge* (RISK) (Baker & Goudie, 2010) bahwa serangan dari *insider* menduduki peringkat ke 2.

ISSN: 2302-3805



Gambar 2 Prosentase serangan insider (Verizon, 2010)

Oleh karena itu diperlukan metode pengamanan jaringan salah satunya dengan menggunakan Virtual Private Network (VPN). VPN biasanya digunakan untuk menghubungkan user atau *site* external ke dalam sistem internal dengan membuat terowongan *(tunnel)* dan enkripsi data, tetapi dalam kasus ini VPN akan digunakan juga untuk mengamankan jaringan internal perusahaan. Jaringan Enterprise adalah jaringan berskala kecil, sedang, ataupun besar yang didalamnya terdapat sistem yang dibangun dengan tujuan untuk memenuhi kebutuhan pengguna internal dalam mengakses aplikasi intranet, extranet, dan remote sistem (Schudel & Smith, 2007). Sistem keamanan berbasis VPN yang dapat digunakan di dalam perusahaan dengan kompleksitas yang cukup tinggi dan mengacu pada pemenuhan dalam jaringan enterprise dapat disebut dengan VPN Enterprise.

Tujuan penelitian tesis ini antara lain adalah:
1. Membuat rancangan infrastruktur keamanan jaringan berbasis VPN beserta dengan pengembangan kebijakan yang mengikutinya.
2. Memberikan solusi bagi PT. TE bahwa OpenVPN sebagai salah satu metode VPN yang dapat memenuhi standar ISO/IEC 27002:2005 sehingga layak untuk di implementasikan dan bisa mengurangi resiko yang diakibatkan oleh kondisi jaringan yang tidak aman.

Diharapkan hasil penelitian ini dapat memberi kontribusi yang signifikan terhadap peningkatan kinerja khususnya keamanan jaringan yang mendukung dalam proses pertukaran informasi di PT. TE dengan beberapa batasan penelitian ini adalah sebagai berikut:
1. Kasus yang diamati yaitu aktifitas transaksi data yang terjadi di lingkungan internal perusahaan PT. TE, khususnya pada jaringan LAN.
2. OpenVPN akan digunakan sebagai implementator keamanan jaringan berbasis open source.
3. Proses analisa dan kajian menggunakan dua standar yaitu ISO/IEC 27002:2005 untuk *compliance* dan NIST SP 800-115 untuk *testing.* Dikarenakan besarnya cakupan bahasan yang terdapat di dalam standar dan ketersediaan waktu yang ada maka penelitian ini menggunakan 2 kategori ISO/IEC 27002:2005 yaitu: Network Security Management (10.6); Network Access Control (11.4), dan menggunakan 2 teknik testing NIST SP 800-115 yaitu: Ruleset Review (3.3); Network Sniffing (3.5)
4. Metode pengamanan di titik beratkan pada konsep keamanan jaringan yang mencakup desain topologi jaringan, teknologi serta kebijakan keamanan yang digunakan.
5. Proof-Of-Concept (POC) dilakukan untuk menguji secara teknis, dan audit internal untuk mengevaluasi kebijakan.

2. Tinjauan Pustaka

Keamanan jaringan enterprise tentunya memiliki cakupan yang luas ditinjau dari sisi desain, kebijakan maupun pelaksanaannya. Tergantung fokus dari pendekatan kebijakan keamanan yang digunakan. Pada penelitian ini sesuai dengan ruang lingkup yang sudah ditentukan difokuskan pada penggunakan VPN sebagai salah satu metode pengamanan data baik digunakan pada jaringan internal maupun external. Dibawah ini adalah beberapa penelitian yang mana mempunyai keterkaitan dengan penelitian yang dilakukan oleh penulis.

Byeong-Ho Kang dan Maricel O. Balitanas (2009), menjelaskan bahwa keamanan data memainkan peranan penting di era bisnis modern yang proses transaksinya banyak menggunakan internet dan perangkat nirkabel. Penelitian yang dilakukan menyajikan kerentanan keamanan yang ditemukan di VPN dengan menggunakan IPSec serta rekomendasi kebijakan dalam penggunaan VPN sebagai metode pengamanan. Kebijakan yang disarankan adalah dengan implementasi VPN dengan konsentrator IPSec untuk karyawan, konsultan, kontraktor atau vendor dan para pekerja lainnya termasuk semua staff atau personel yang berhubungan dengan pihak ketiga kesemuannya memanfaatkan jaringan VPN untuk mengakses sumber daya yang ada di perusahaan.

Advance Security Architecture for Multi-Homed Virtual Private Network, jurnal ilmiah yang ditulis oleh M. Sreedevi dan R. Seshari (2011) menyebutkan bahwa VPN dapat memberikan dukungan jaringan yang sangat handal sehingga dapat menjadi solusi yang membawa tingkat keamanan pada tingkat yang baru. Metode multi-homed VPN digunakan untuk menghubungkan jaringan privat ke jaringan publik melalui penyedia layanan internet(ISP) yang berbeda. Sehingga kegagalan yang disebabkan dari setiap ISP dapat diminimalkan dengan koneksi ISP yang lain akan menjaga jaringan tetap tersambung. Makalah ini mengangkat penggunaan *Advanced Encryption Standard* (AES) sebagai metode enkripsi data pada multi-homed VPN, serta metode keamanan yang ada pada saat ini seperti firewall, IPSec, serta keuntungan yang didapat.

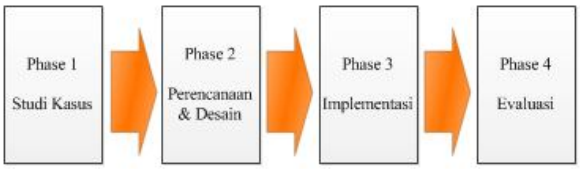
ISSN: 2302-3805

Ritu Malik dan Rupali Syal (2010) dalam jurnal berjudul Perfomance Analysis of IP Security VPN mengangkat tentang penggunaan IPSec sebagai protokol untuk mengamankan komunikasi berbasis Internet Protocol (IP) dengan otentikasi dan enkripsi. IPSec telah menjadi metode pengamanan yang paling umum dan mempunyai mekanisme yang luas untuk digunakan dalam VPN. Tulisan dalam jurnal ini lebih khusus membahas analisis dari penggunaan IPSec VPN untuk mengamankan jaringan komunikasi pada aplikasi video conference.

Dari ketiga tinjauan diatas dapat diketahui bahwa penggunaan VPN dengan proses otentikasi dan enkripsinya dapat memperkuat atau mengamankan jaringan komunikasi sehingga data dapat dijamin validitasnya. IPSec yang dikembangkan oleh *Internet Engineering Task force* (IETF) menjadi protokol yang umum digunakan dalam implementasi VPN. Sedangkan pada penelitian kali ini solusi VPN menggunakan OpenVPN dengan berbasis protokol SSL/TLS yang menawarkan berbagai keuntungan selain yang ditawarkan daripada IPSec.

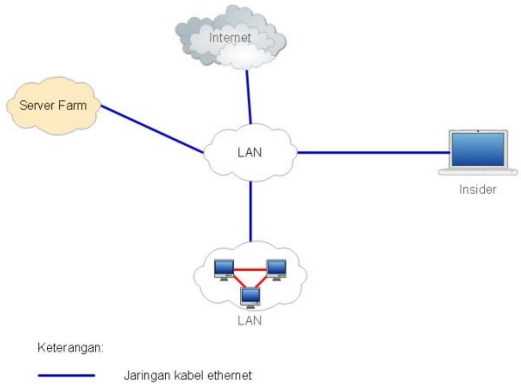
3. Metode Penelitian

Adapun metodologi yang digunakan dalam penelitian ini meliputi beberapa kegiatan seperti yang terlihat pada Gambar 3. Dimana terdapat 4 tahapan penelitian, yaitu: 1) Studi kasus; 2) Perencanaan dan Desain; 3) Implementasi; 4) Evaluasi.



Gambar 3 Diagram phase metode penelitian

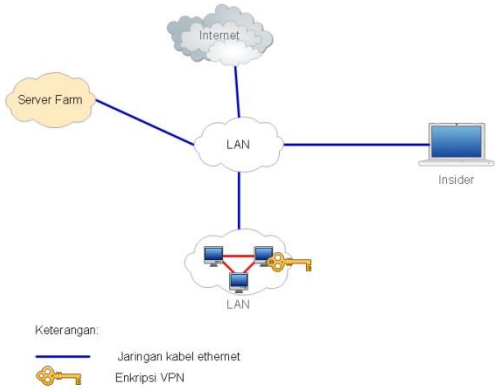
1) Studi Kasus
   Pada tahapan ini dilakukan proses pengamatan dan pengambilan data dari kondisi jaringan existing PT. TE melalui eksperimen dengan menggunakan metode network sniffing yang mengacu pada teknik dari standar NIST SP 800-115, mencakup di dalamnya proses pencarian atau pembuktian ancaman seperti yang ditunjukkan dengan model. Hasil dari phase ini adalah data yang menunjukkan bahwa sistem jaringan komputer yang ada sekarang tidaklah aman.



Gambar 4 Model penyerangan

2) Perencanaan dan Desain
   Melakukan perencanaan secara sistematis dengan menyiapkan rancangan skema desain sistem keamanan jaringan berbasis VPN yang disesuaikan dengan topologi jaringan eksisting beserta *policy* yang digunakan sebagai *guideline* dalam melakukan konfigurasi dan kebijakan operasional penggunaan untuk pengguna. Dalam pembuatan *policy* mengacu pada pemenuhan 2 kategori standar ISO/IEC 27002:2005 yaitu: Network Security Management (10.6); Network Access Control (11.4).
3) Implementasi
   Pada tahapan ini dilakukan proses implementasi sistem yang telah direncanakan beserta *policy* yang telah di desain sebelumnya dengan metode POC. Seluruh rangkaian aktivitas yang dilakukan dalam penelitian ini dilaksanakan di lingkungan PT. TE termasuk didalamnya perangkat server dan komputer pengguna.
4) Evaluasi
   Melakukan review dengan menggunakan metode network sniffing yang mengacu pada teknik dari standar NIST SP 800-115 seperti yang terlihat pada model Gambar 5. data diharapkan dapat menunjukkan bahwa sistem yang di desain dan di implementasikan benar-benar dapat berfungsi dengan baik sehingga dapat mencapai tujuan yang telah ditetapkan. Evaluasi juga akan dilakukan dengan menggunakan metode internal audit yang dilaksanakan oleh tim Management Representative (MR) dan internal auditor yang ditunjuk.

ISSN: 2302-3805



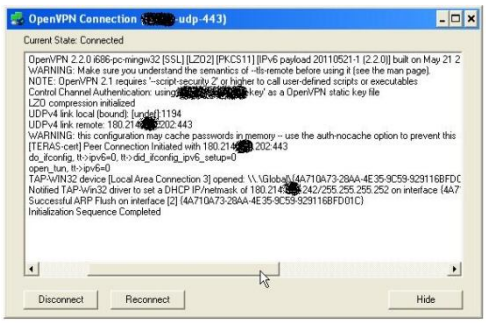
Gambar 5 Model evaluasi implementasi VPN

4. Hasil dan Pembahasan

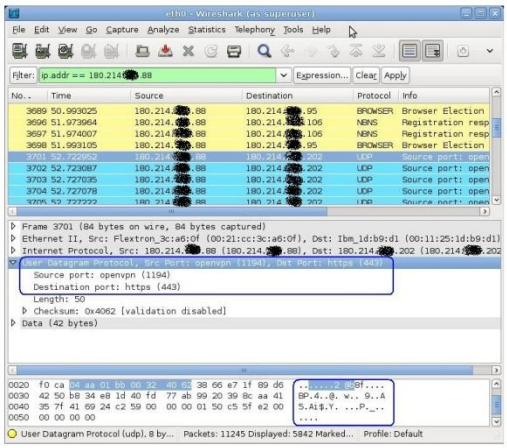
Setelah pada proses desain dan perancangan sistem selesai dibuat, maka peneliti melakukan POC sebagai salah satu metode pembuktian, sebelum pada akhirnya sistem benar-benar siap digunakan secara nyata pada kondisi kerja yang sebenarnya. POC dilakukan dengan sedapat mungkin tidak mengganggu sistem jaringan existing, namun tetap menggunakan situs-situs real sebagai bahan uji coba. Tahapan yang akan dievaluasi oleh peneliti melalui POC ini adalah mulai pada pengguna melakukan koneksi VPN kemudian melakukan aktifitas dengan melakukan akses atau transaksi data dan ketika pengguna telah selesai menggunakan layanan koneksi VPN, serta evaluasi penggunaan *policy* yang telah dibuat sebelumnya. Data yang tertuang dalam penelitian ini tersaji dalam gambar, karena faktor privacy dan keamanan maka sebagian informasi yang disajikan sebagian akan dikaburkan.

Berikut merupakan hasil capture yang memperlihatkan bahwa sistem layanan VPN yang digunakan di dalam POC, terbagi dalam 3 sesi yaitu: 1) Opening Session; 2) Running Session; 3) Closing Session.

1) Opening Session
   Opening session adalah proses awal dimana komputer pengguna sudah menjadi target penyerangan oleh intruder kemudian melakukan inisiasi koneksi dengan layanan VPN seperti pada Gambar 6. Dapat terlihat bahwa meskipun sudah menjadi target *sniffing* oleh intruder, komputer pengguna masih dapat dengan baik melakukan inisiasi VPN sampai pada mendapatkan alokasi IP VPN. Pada Gambar 7 adalah gambaran dimana semua traffic pada saat inisiasi dimulaipun sudah terenkripsi oleh VPN.

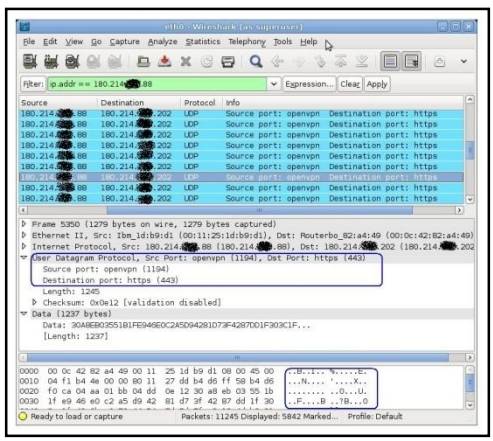


Gambar 6 Opening session OpenVPN client



Gambar 7 Data sniffing pada opening session

2) Running Session
   Running session adalah proses dimana pengguna telah berhasil menggunakan layanan VPN, sehingga semua lalu lintas percakapan data sepenuhnya terlindungi di dalam tunnel dan terenkripsi. Apabila intruder melakukan aktifitas *sniffing*, maka akan didapatkan data yang sudah dalam keadaan teracak atau terenkripsi seperti yang terlihat pada Gambar 8, sehingga meskipun berhasil mendapatkan data-data, namun demikian data tersebut menjadi tidak berguna.

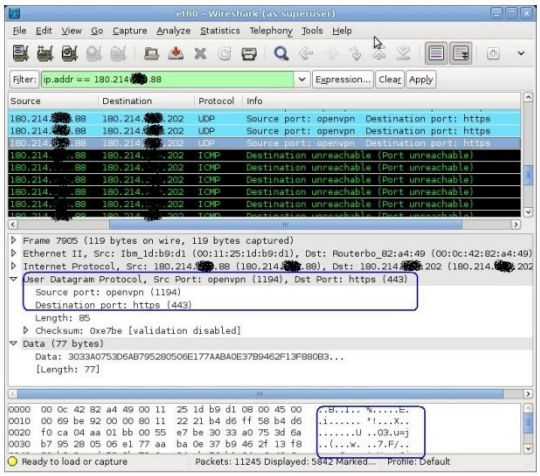


Gambar 8 Data sniffing pada running session

3) Closing Session

ISSN: 2302-3805

Closing session adalah proses dimana komputer pengguna telah selesai melakukan aktifitasnya dan kemudian mengakhiri penggunaan layanan VPN. Seperti yang terlihat dalam Gambar 9 bahwa sampai pada koneksi VPN terakhirpun data masih dalam terbungkus di dalam tunnel dan terenkripsi.

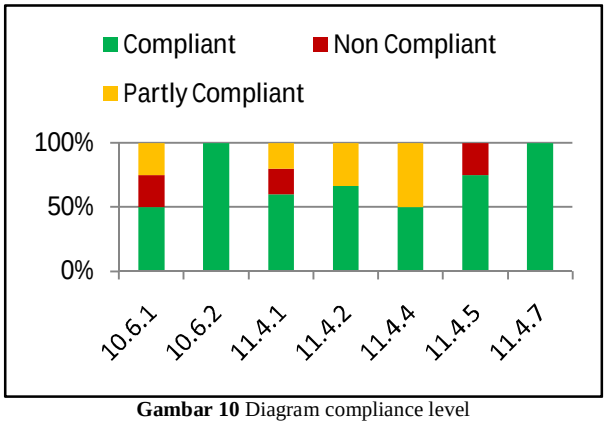


Gambar 9 Data sniffing pada closing session

Dari hasil evaluasi teknis yang telah dipaparkan diatas, dapat diketahui bahwa penggunaan sistem VPN yang telah dirancang sebelumnya dapat berjalan dengan baik. Terlihat dari POC yang dilakukan, serta evaluasi dengan menggunakan metode *network sniffing*, intruder tidak bisa mendapatkan informasi rahasia seperti username dan password dengan mudah. Sangat berbeda ketika pengguna dalam kondisi tidak menggunakan VPN, data-data rahasia tersebut dapat dengan mudah didapatkan. menggunakan VPN, data-data rahasia tersebut dapat dengan mudah didapatkan. Untuk memperkuat hasil analisa dalam evaluasi, hasil pre-implementasi dengan POC diaudit secara internal oleh tim MR dan internal auditor.

Dari hasil internal audit yang dilakukan dapat diperoleh data, bahwa policy yang telah dibuat dapat dibedakan dalam 3 (tiga) kategori pemenuhan yaitu:

1) *Compliant*, menjelaskan bahwa policy yang dibuat dapat memenuhi kriteria dalam kategori ISO/IEC 27002:2005 dan dapat berjalan dengan baik.
2) *Non Compliant*, menjelaskan bahwa policy yang dibuat belum dapat diimplementasikan karena faktor teknis ataupun non-teknis.
3) *Partly Compliant*, menjelaskan bahwa policy yang dibuat belum memenuhi kriteria dalam kategori ISO/IEC 27002:2005, atau policy sudah memenuhi syarat tetapi dalam pelaksanaannya masih belum komitmen atau konsisten.

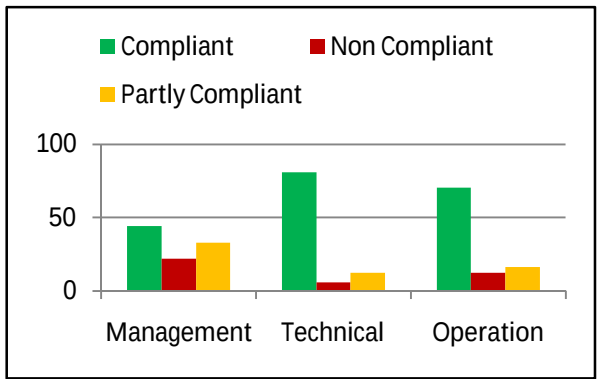


Gambar 10 Diagram compliance level

Dari yang disajikan dalam Gambar 10 menunjukkan bahwa policy yang dibuat pada sub-kategori 10.6.2 dan 11.4.7, 100% policy dapat berjalan dengan baik serta memenuhi syarat dari standar ISO/IEC 27002:2005. Dari semua policy yang telah dibuat terlihat dapat diterima dan dapat berjalan dengan baik secara teknis maupun pada level kebijakan, hal ini ditunjukkan dengan tingkat pemenuhan yang berada pada level 50% keatas pada hasil audit internal yang dilakukan dari masing-masing sub-kategori.

Analisis selanjutnya adalah dengan melihat hasil pemenuhan policy yang dibuat dengan scope area pada organisasi, terlihat pada Gambar 11 bahwa dari 24 policy yang dibuat dibedakan dalam 3 (tiga) scope area organisasi (ISO/IEC 27002:2005) yaitu:

1) Management, yaitu kontrol yang didalamnya terdapat pengaturan atau kebijakan terkait dengan organisasi secara keseluruhan.
2) Technical, yaitu kontrol yang didalamnya terdapat pengaturan konfigurasi teknis.
3) Operation, yaitu kontrol yang didalamnya terdapat pengaturan pada level operasional pengguna.



Gambar 11 Scope area level

5. Kesimpulan dan Saran

Dari hasil penelitian yang telah dilakukan, maka didapatkan beberapa kesimpulan sebagai berikut :

1) Berdasarkan hasil penelitian pada jaringan internal PT. TE dengan menggunakan teknik testing Network Sniffing dan Review Technique dari standar NIST

ISSN: 2302-3805

SP800-115, dapat disimpulkan bahwa kondisi jaringan internal PT. TE masih belum aman, sehingga masih mempunyai potensi terjadinya proses penyadapan data oleh *intruder*. Maka melalui analisa dan kajian yang dilakukan terhadap permasalahan yang terjadi, diputuskan untuk membuat rancangan infrastruktur sistem keamanan jaringan dengan teknologi VPN dengan OpenVPN sebagai implementator server VPN.

2) Rancangan sistem VPN yang dibangun dengan menggunakan OpenVPN, selain dapat mengatasi masalah yang ada juga harus dapat mengacu pada kriteria dalam standar keamanan ISO/IEC 27002 dalam bentuk sebuah kebijakan yang mengatur konfigurasi dan penggunaan sumber daya perusahaan. Sistem jaringan yang dirancang telah disimulasikan secara nyata dengan melakukan *Proof-of-Concept* di internal perusahaan dan dapat berjalan dengan baik serta policy yang diterapkan juga dapat memenuhi kriteria dalam standar ISO/IEC 27002:2005. Sistem ini dapat bermanfaat bagi PT. TE karena memiliki kemampuan sebagai berikut:
   a. Dapat digunakan untuk memperkuat keamanan jaringan selain daripada penggunaan metode pengamanan yang lain, sehingga secara psikologis dapat menambah rasa aman dan percaya diri dalam melakukan transaksi data.
   b. Dapat digunakan sebagai *remote access* VPN untuk karyawan PT. TE yang sedang dinas di luar kantor dengan membuat jalur komunikasi yang lebih aman dan terenkripsi.

Desain yang dibuat pada penelitian ini, agar dapat dijadikan landasan dalam perancangan sebuah sistem enterprise di lingkungan PT. TE sehingga dapat menjadi salah satu bagian dalam cetak biru khususnya untuk kategori keamanan jaringan yang siap untuk diterapkan di PT. TE. Agar kajian terhadap penggunaan OpenVPN dalam pembangunan sistem keamanan jaringan dengan teknologi VPN dapat lebih komprehensif, disarankan perlu adanya penelitian yang mengulas apakah OpenVPN ini juga dapat memenuhi standar TI yang lain seperti Cobit 4.1 dan ITIL V3 baik secara teknis dan kebijakan.

Daftar Pustaka

[1] Baker, W., Goudie, M., 14 November 2011, *Data Breach Investigations Report*, http://www.verizonbusiness.com/Products/security/dbir/
[2] Byeong-Ho, K., Maricel, O. B., 2009, Vulnerabilities of VPN using IPSec and Defensive Measures. *International Journal of Advanced Science and Technology, Volume 8*
[3] Sreedevi, M., Seshadri, R., 2011, Advance Security Architecture for Multi Homed Virtual Private Networks. *American Journal of Scientific Research*(ISSN: 1450-223X, Issue 22, 2011)
[4] Richardson, R., 14 November 2011, *CSI Computer Crime and Security Survey.* http://www.gocsi.com
[5] Ritu, M., Rupali, S., 2010, Performance Analysis of IP Security VPN. *International Journal of Computer Applications, Volume 8 No.4*

Biodata Penulis

Agustinus Donny Mahendra, S.Kom, memperoleh gelar Sarjana Komputer (S.Kom), Program Studi Teknik Informatika STMIK Amikom, lulus tahun 2006. Saat ini sedang menyelesaikan studi di Magister Teknik Informatika STMIK Amikom Yogyakarta.

Dr. Ema Utami, S.Si, M.Kom, memperoleh gelar Sarjana Sains (S.Si) dari Program Studi Ilmu Komputer UGM pada tahun 1997. Tahun 2002 memperoleh gelar Magister Komputer (M.Kom) dengan predikat cumlaude dari Program Pascasarjana Ilmu Komputer UGM. Tahun 2010 memperoleh gelar Doktor dari Program Doktor Ilmu Komputer UGM. Sejak 1998 menjadi Staff Pengajar di STMIK AMIKOM Yogyakarta dan sejak 2010 menjadi Wakil Direktur I Bidang Akademik Program Pascasarjana STMIK AMIKOM Yogyakarta.

Ir. Abas Ali Pangera, M.Kom, memperoleh gelar Sarjana Teknik (Ir) dari Program Studi Teknik Elektro UGM pada tahun 1986. Tahun 2004 memperoleh gelar Magister Komputer (M.Kom) dari Program Pascasarjana Ilmu Komputer UGM.