# Perancangan *Security Technology Architecture* PT. "N" Menggunakan Kerangka Kerja *Enterprise Security Architecture*

**Sriwisnu Noloadi**

Program Studi Magister Sistem Informasi
Fakultas Pascasarjana
Universitas Komputer Indonesia

## ABSTRAK

*Arsitektur teknologi keamanan pada sebuah enterprise merupakan bagian dari dukungan sistem bisnis perusahaan yang sangat diperlukan, adanya kemungkinan fraud, gangguan sistem termasuk ancaman virus dan spam merupakan alasan diperlukannya teknologi keamanan yang handal bagi perusahaan, berdasarkan kondisi perusahaan saat ini teknologi keamanan yang memadai sangat mendesak diperlukan oleh PT "N" dengan tujuan pengoperasian sistem teknologi informasi yang mendukung proses bisnis perusahaan dalam kaitannya dengan ketersediaan data dan informasi yang aman. Kerangka kerja ESA (Enterprise System Architecture) dari NAC (Network Applications Consortium) digunakan untuk penyusunan dan perancangan Security Technology Architecture melalui 4 (empat) tahapan penting yaitu: menyusun kerangka kerja konseptual, arsitektur konseptual, arsitektur logis dan arsitektur fisik. Layanan penerapan Security Technology Architecture mencakup kontrol akses, proteksi batasan fisik, deteksi, kontrol isi informasi, auditing dan kriptografi. Hasil akhir menunjukkan bahwa yang paling cocok dari penyusunan dan penerapan Security Technology Architecture bagi perusahaan adalah dengan mengusulkan model keamanan yang yang mencakup bisnis, sistem informasi, dan arsitektur teknologi dengan mengandalkan dasar-dasar teknis yang direkomendasikan dan bisa diterapkan di telekomunikasi dan perusahaan pada umumnya.*

*Kata kunci: Security Technology Architecture, ESA, NAC, TOGAF, NIST*

## 1. Latar Belakang

Trend teknologi informasi yang berkembang sangat pesat berpengaruh terhadap strategi dan kebijakan perusahaan yang berorientasi untuk mencari keuntungan seperti halnya perusahaan yang bergerak dibidang telekomunikasi. PT. "N" Telepon Selular adalah salah satu perusahaan operator telekomunikasi yang bergerak dibidang pelayanan voice, SMS dan data internet yang dalam mengembangkan bisnisnya, perusahaan ini terus mengikuti trend teknologi informasi demi memenuhi kepuasan pelanggan yang berjumlah lebih dari 15 juta pelanggan. Tingkat kompetisi bisnis telekomunikasi yang tinggi dalam meningkatkan jumlah pelanggan menuntut perusahaan untuk menyediakan layanan yang memuaskan, untuk mencapai tujuan ini perusahaan harus bisa menjaga sistem dengan baik agar tidak terjadi *fraud,* kesalahan atau gangguan terhadap sistem yang sedang berjalan dan dapat mempengaruhi aktifitas bisnis perusahaan, sehingga kebutuhan akan sistem keamanan yang handal dan terintegrasi sangat dibutuhkan oleh perusahaan.

Salah satu penemuan masalah keamanan berupa *fact finding* yang bisa menimbulkan ancaman keamanan adalah begitu mudahnya siapapun *(anonymous user)* mendapatkan akses kedalam sistem jaringan perusahaan seperti

mudahnya mendapat alamat internet protokol melalui akses wireless sehingga jika penyusup mengetahu target IP yang diakses akan sangat mudah mendapatkan login prompt, hal ini sangat rentan akan proses eksploitasi yang dilakukan oleh orang yang mencoba akses illegal melalui jalur ini.

Dari permasalahan diatas maka perlu disusun suatu rumusan permasalahan yang sedang dihadapi oleh perusahaan terkait teknologi keamanan, yaitu:

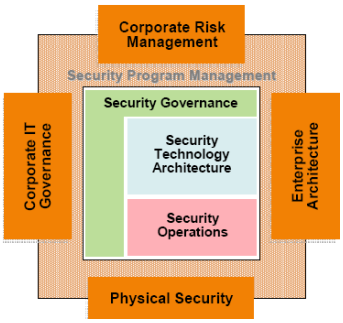
- Akses kedalam sistem jaringan perusahaan masih sangat rentan seperti mudahnya mendapat alamat internet protokol baik melalui *wireless connection* maupun melalui *physical connection* sehingga sistem rentan mendapatkan kesalahan *(fraud) dan* gangguan keamanan bagi perusahaan terbukti dengan mudahnya mendapatkan *shell prompt* kedalam sistem yang kritikal seperti sistem biling dan lain sebagainya.
- Dari permasalahan pertama diatas masalah berikutnya yang timbul adalah bagaimana sebenarnya profil risiko keamanan teknologi informasi di perusahaan yang bisa mengakibatkan perusahaan mendapatkan potensi dampak dari risiko keamanan.
- Bagaimana perusahaan menyusun S*ecurity Technology Architecture* agar perusahaan mempunyai solusi yang tepat untuk meningkatkan keamanan yang memadai.

Dengan mendalami permasalahan diatas, dan mencari solusi yang tepat maka perusahaan bisa mencapai suatu tujuan terkait dengan teknologi keamanan yang diharapkan seperti:

- Perusahaan akan memperoleh solusi teknologi keamanan yang tepat dan memadai untuk mengatasi timbulnya *fraud,* kesalahan dan gangguan sistem dengan cara memberikan gambaran yang jelas tentang arsitektur teknologi keamanan dan kaitannya dengan fasilitas infrastruktur yang dimiliki perusahaan.
- Perusahaan bisa mengetahui dan menganalisa profil risiko keamanan yang dimiliki dan diterapkan kedala
- Perusahaan memiliki ipengukuran risiko dan dampak risiko keamanan yang bisa menimbulkan dampak bisnis perusahaan.
- Perusahaan mampu menyusun dan merancang S*ecurity Technology Architecture* yang tepat dan memadai guna memitigasi risiko dan mengatasi ancaman-ancaman bagi keamanan IT perusahaan sehingga berguna bagi perusahaan dimasa mendatang

## 2. Enterprise Security Architecture

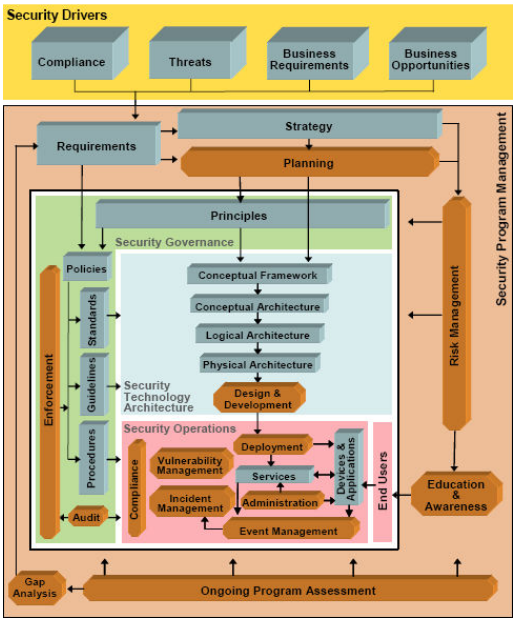
Kerangka kerja *Enterprise Security Architecture* (ESA) dari NAC harus dipahami dalam konteks perusahaan besar, dimana hal ini adalah bagian dari program keamanan perusahaan secara keseluruhan, seperti ditunjukan dalam gambar 2.2 yang menggambarkan hubungan didalam kerangka kerja ESA terhadap manajemen risiko perusahaan, tata kelola teknologi informasi, arsitektur enterprise dan keamanan fisik.




Gambar 2.1 Konteks *Enterprise Security*

Kerangka yang lebih lengkap dalam konteks *Enterprise Security* suatu perusahaan menjelaskan bagian-bagian penting yang lebih dalam tentang program *Enterprise Security.* Kerangka kerja ini dimulai dari *security driver* pada bagian atas yang menunjukan sumber-sumber utama persyaratan keamanan bagi kebutuhan keamanan perusahaan yang perlu diidentifikasi satu per satu, sumber inti dari kebutuhan area bisnis yaitu mempunyai tingkat layanan *(service-level)* yang sesuai dengan layanan yang diberikan kepada pelanggan dan mendapat kentungan dari peluang bisnis yang baru, selanjutnya kebutuhan dari luar adalah termasuk ancaman keamanan, legasi serta *regulatory compliance* dari pemerintah.

Gambar berikut ini menunjukan skema yang lengkap suatu kerangka kerja program *enterprise security,* didalamnya ada bagian tentang *Security Technology Architecture* yang terdiri dari komponen-komponen *conceptual framework, conceptual architecture, logical architecture* dan *physical architecture*.




Gambar 2.2 Enterprise Security Programme

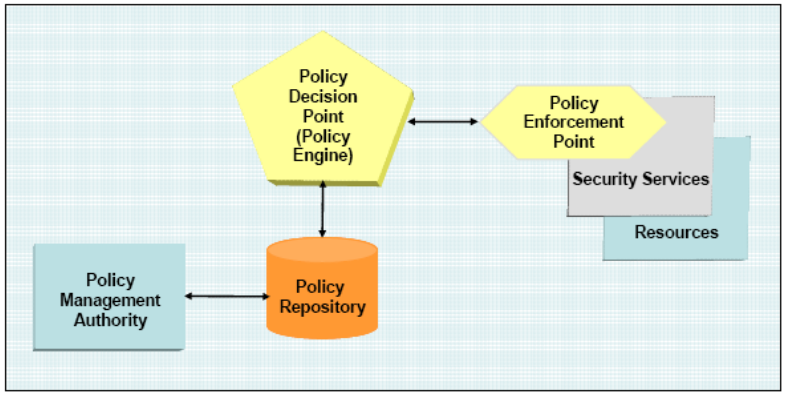
Terkait dengan Technology Architecture yaitu menyangkut hal-hal sebagai berikut:

- *Conceptual framework:* kerangka kerja konseptual berbasis manajemen pelayanan keamanan.
- *Conceptual architecture:* struktur konseptual untuk manajemen pengambilan keputusan dan penegakan kebijakan layanan keamanan.
- *Logical architecture:* menyediakan struktur secara terperinci pada komponen logis untuk layanan keamanan.
- *Physical architecture:* Arsitektur fisikyang memberikan fungsi yang diperlukan dan memberikan kinerja yang baik, dan handal.
- *Design/development:* panduan atau template yang dapat digunakan kembali, dalam pemanfaatan yang efektif dan integrasi aplikasi ke lingkungan ESA.

## 2.1 Policy Driven Security Conceptual Framework

Kerangka kerja konseptual dalam jurnal *"Enterprise Security Architecture* [1]*"* adalah sebagai salah satu tahapan dalam menyusun *Security Technology Architecture* merupakan arsitektur layanan keamanan *(security services)* yang menjelaskan tentang keamanan berbasis kebijakan *(Policy Driven Security),* dimana cara kerja kerangka tersebut adalah dengan menyatakan

suatu representasi kebijakan yang disimpan di dalam *repository* untuk proses *runtime* yang bertujuan menjalankan kebijakan yang diterapkan, skema kerangka kerja konseptual menjelaskan tentang langkah-langkah secara konseptual dalam menerapkan policy didalam sistem computer, gambar 2.3 dibawah ini menggambarkan tentang komponen utama dari dari model kerangka kerja konseptual keamanan berbasis kebijakan.



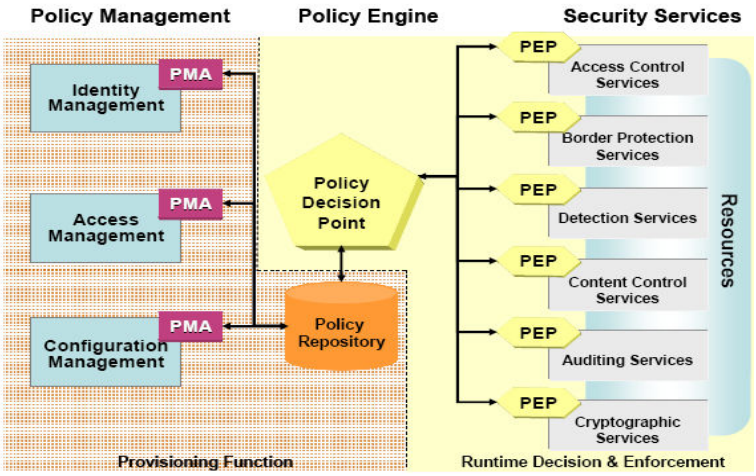

Gambar 2.3 framework konseptual keamanan berbasis kebijakan

Penjelasan mengenai skema kerangka kerja konseptual diatas adalah sebagai berikut:

- *Policy Management Authority* (PMA) adalah entitas aplikasi yang membentuk atau menciptakan representasi kebijakan elektronik melalui konsol kebijakan dinyatakan dengan *eXtensible Markup Language* (XML) berupa entri direktori, file konfigurasi..
- *Policy Decision Point* (PDP), PDP bertugas membuat keputusan kebijakan *runtime* atas permintaan *Policy Enforcement Point* (PEP).
- *Policy Repository,* repositori merupakan direktori berisi sarana layanan kebijakan.
- *Policy Enforcement Point (*PEP), PEP memberlakukan kebijakan saat *runtime*, berdasarkan keputusan kebijakan dari PDP. Fungsi PEP terintegrasi dengan layanan keamanan.
- *Security Services,* merupakan layanan keamanan terhadap *resources* atau aset-aset perangkat keras dan perangkat lunak di IT.
- *Resources* adalah aset IT sebagai target akses.

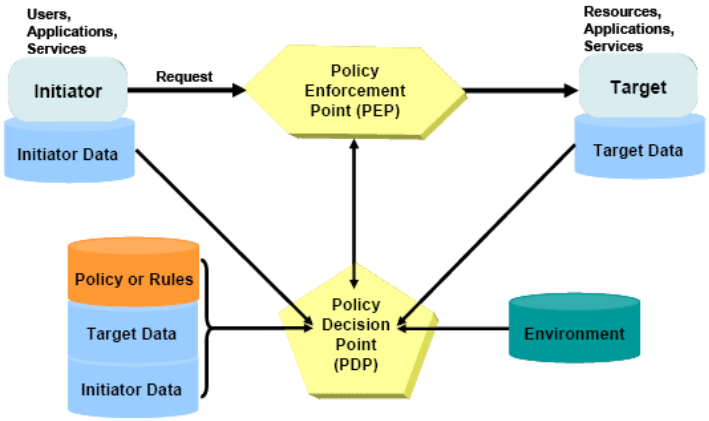
## 2.2 Arsitektur Konseptual Keamanan Berbasis Kebijakan

Arsitektur konseptual dimulai dengan melakukan dekomposisi kebijakan pengelolaan dan layanan keamanan komponen dari kerangka konseptual untuk suatu layanan tertentu, representasinya dibagi dalam tiga bagian yaitu *Policy Management, Policy Engine* dan *Security Services* seperti yang terlihat secara lengkap dalam gambar 2.4 sebagai berikut:




Gambar 2.4 Arsitektur konseptual keamanan berbasis kebijakan

Arsitektur konseptual diatas terdiri dari 3 bagian yaitu *Policy Management, Policy Engine* dan *Security Services*, bagian *Policy Management* terdiri atas *Identity Management, Access Management* dan *Configuration Management.* Porsi *Policy Engine* merupakan suatu *Policy Decision Point*, untuk porsi Security Services, layanan ini terdiri dari *Access Control Services, Border Protection Services, Detection Services, Content Control Services, Auditing Services,* dan *Cryptographic Services.* Untuk menjelaskan PDP/PEP secara detil dalam arsitektur konseptual diuraikan dalam gambar berikut ini:




Gambar 2.5 Model PDP/PEP dalam arsitektur konseptual

Dari gambar PDP/PEP di atas mendefinisikan hal-hal sebagai berikut:

- Inisiator: pengguna, aplikasi, atau layanan yang memulai permintaan beberapa target dari sumber daya. Inisiator mungkin berupa kebijakan manajemen administrator, aplikasi, layanan, pengguna akhir atau yang menggunakan aplikasi.
- Target: aplikasi, layanan, atau sumber daya lain yang aksesnya didasarkan pada permintaan yang diarahkan oleh inisiator. Target bisa merupakan repositori kebijakan yang diperbaharui oleh layanan pengaturan kebijakan, atau mungkin menjadi sumber daya yang dioperasikan oleh salah satu layanan keamanan secara *runtime*.

- PEP: berfungsi sebagai penjaga yang menjalankan keputusan kebijakan terhadap target sumber daya.
- PDP: merupakan mesin yang mengevaluasi permintaan terhadap suatu kebijakan atau aturan data dan membuat suatu keputusan tentang kebijakan.

Operasi dasar terkait arsitektur konseptual adalah bahwa inisiator mengajukan suatu permintaan terhadap target, permintaan ini akan menentukan operasi yang akan dilakukan pada target, dan mungkin berisi data yang relevan atau instruksi yang lebih rinci. Permintaan yang dihadapi oleh PEP, dikemas ke dalam keputusan berisi permintaan, dan diteruskan ke dalam PDP dengan tujuan menentukan apakah permintaan tertentu harus diberikan atau ditolak. Untuk membuat keputusan kebijakan, PDP memerlukan informasi-informasi sebagai berikut:

- Data inisiator disimpan di direktori LDAP, yang dibuat dan dikelola oleh layanan manajemen identitas.
- Target data adalah data tentang sumber daya target dan biasanya berhubungan dengan sensitivitas informasi atau klasifikasi suatu konten.
- *Environment data*: mencakup tentang waktu, jalur akses, konteks pengguna sesi, atau konteks transaksi. Jalur akses mungkin menunjukkan keamanan saluran akses atau lokasi pengguna saat ini, misalnya sistem yang terhubung ke jaringan perusahaan dan internet. Lingkungan ini harus mudah diakses oleh PDP untuk membuat suatu keputusan yang diperlukan secepatnya.
- *Policy* atau *Rules:* Kebijakan atau aturan ditujukan untuk membuat keputusan kebijakan tentang permintaan sumber daya tertentu, kebijakan atau aturan ini ditampilkan sebagai suatu repositori kebijakan yang mungkin menjadi layanan direktori. Kombinasi suatu sumber direktori data yang diakses sebagai sebuah direktori virtual, *meta directory*, atau merupakan repositori suatu kebijakan khusus.

# 3. Perencanaan Security Technology Architecture PT "N"

## 3.1 Proses Business Perusahaan

Dari proses observasi di lapangan, perusahaan mempunyai 20 (dua puluh) proses bisnis utama pendukung sistem bisnis perusahaan yang merupakan bisnis proses yang sedang berjalan saat ini.

Tabel 3.1 Daftar bisnis proses utama, fungsi bisnis proses perusahaan serta aplikasi terkait

| No | Nama Bisnis Proses | Fungsi Bisnis Proses | Aplikasi BSS | Aplikasi Non BSS |
|---|---|---|---|---|
| 1 | *Starter Pack Production Process* | Proses untuk menghasilkan kartu perdana SIM | SAP, Carmen, CRM, Provisioning | NE *(Network Element*) |
| 2 | *Voucher Production Process* | Proses untuk menghasilkan nomor *voucher* dan nilai pulsanya untuk SIM *card* | SAP, Carmen | Voucher Management |
| 3 | *Sales Starter Pack Process* | Proses memasarkan kartu perdana kepada customer dalam meningkatkan jumlah pelanggan | CRM, SAP, Carmen | - |
| 4 | *Sales Voucher Process* | Proses untuk memasarkan voucher fisik pulsa isi ulang SIM *card* customer | CRM, SAP, Carmen | - |
| 5 | *Sales Electronic Recharge Process* | Proses untuk memasarkan isi ulang pulsa secara elektronis | SAP | Utiba, 3rd Party Gateway |
| 6 | *Retail Prepaid Activation and Deactivation Process* | Proses aktivasi dan deaktivasi kartu prabayar | Message Middleware, ODS, Carmen, Provisioning, CRM | Prepaid Registration System, OCS |
| 7 | *Postpaid Activation and Deactivation Process* | Proses aktivasi dan deaktivasi pelanggan pasca bayar | CCBS, EAI, Carmen, CRM, Provisioning, Message Middleware | OCS |

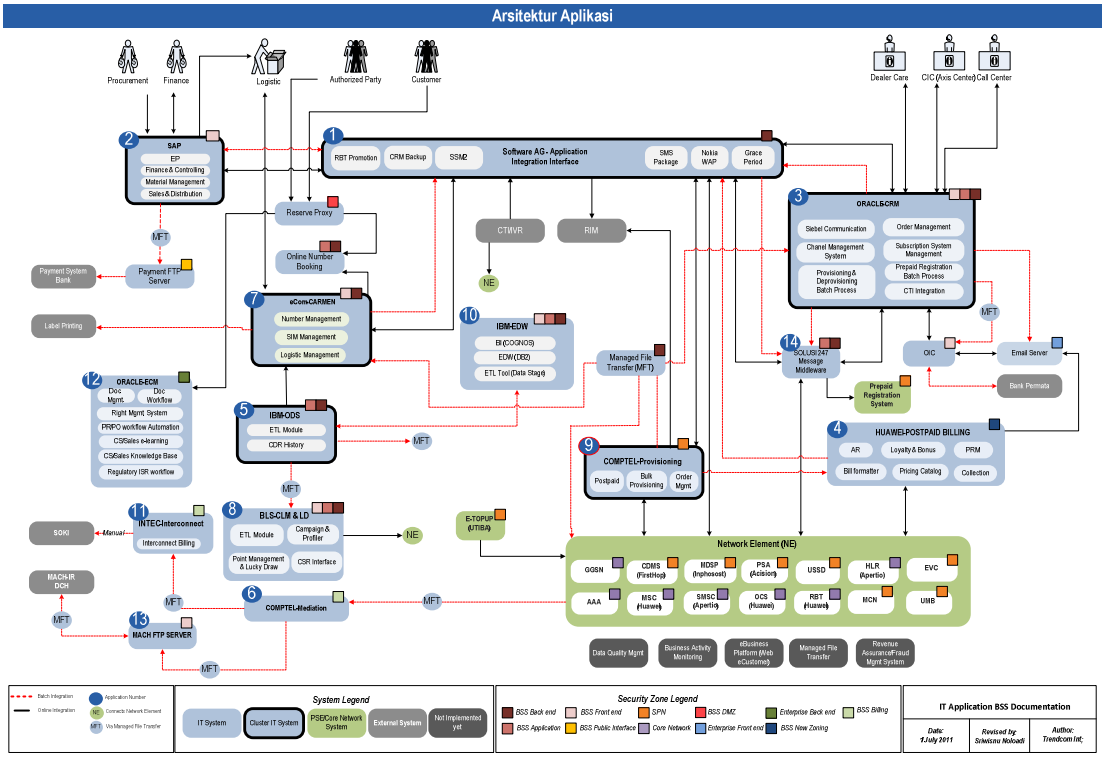
| | | | | |
|---|---|---|---|---|
| 8 | *Subscriber Trouble Ticketing* | Proses untuk menangani masalah komunikasi handphone pelanggan | CRM | Email Server |
| 9 | *Order Handling Process* | Proses untuk menangani pemesanan kartu SIM | CRM, EAI, Carmen, Provisioning, SAP | OCS |
| 10 | *Sales Starter Pack (Shop) Process* | Proses pemasaran kartu perdana SIM *card* kepada distributor | Carmen, SAP, CRM | |
| 11 | *Sales Voucher (Shop) Process* | Proses pemasaran *voucher* fisik pulsa isi ulang kepada distributor | Carmen, SAP, CRM | |
| 12 | *Sales Electronic Voucher (Shop)* | Proses pemasaran *voucher* elektronis pulsa isi ulang | CRM, SAP | |
| 13 | *Sales Bundling Package Process* | Proses pemasaran paket *bundle* | Carmen, SAP, CRM | |
| 14 | *Billing Process* | Proses untuk *customer care* dan *billing system* | CCBS, Message Middleware, SAP | OCS, Email Server |
| 15 | *Payment Process* | Proses pembayaran tagihan pelanggan | CCBS, Provisioning, Message Middleware, SAP | Payment Channel, OCS |
| 16 | *Collection Process* | Proses *collection* data percakapan, sms dan internet | CCBS, Provisioning, SAP | OCS |
| 17 | *Revenue Accounting* | Proses penghitungan pendapatan perusahaan | CRM, CCBS, Interconnect, ODS, SAP, PRM | MSC, OCS, Utiba, 3rd Party Gateway |
| 18 | *Interconnect Settlement* | Proses perhitungan pemakaian pulsa untuk *interconnect* antar operator | Mediation, Interconnect | SOKI Server |
| 19 | *International Roaming Settlement* | Proses perhitungan pemakaian roaming internasional | Mediation, PRM, SAP | Mach, OCS |
| 20 | *Loyalty Management* | Proses untuk *loyalty* dan hadiah untuk *customer* | ODS, Interconnect, Message Middleware, OCS, CRM | Other Data Source |

## 3.2 Arsitektur Aplikasi saat ini

Arsitektur aplikasi sebagai pendukung sistem bisnis perusahaan merupakan aplikasi-aplikasi yang terintegrasi, hasil observasi di lapangan yang dilakukan secara mendalam pada area yang berhubungan dengan proses bisnis utama terdiri dari beberapa macam aplikasi IT-BSS pendukung sistem bisnis perusahaan, yaitu: EAI, SAP, CRM, CCBS, ODS, Mediation, Carmen, CLM&LD, Provisioning, EDW, Interconnect, ECM, IR Settlement dan Message Middleware. Untuk membuktikan bahwa aplikasi-aplikasi tersebut merupakan pendukung sistem bisnis perusahaan melalui proses bisnis yang telah dijabarkan. Aplikasi ini terintegrasi dan saling berkomunikasi satu sama lain baik melalui aplikasi EAI ataupun secara langsung dari satu aplikasi ke aplikasi yang lain.. EAI merupakan aplikasi enterprise yang bertugas melakukan proses *request* dan *response* untuk menghubungkan aplikasi-aplikasi yang saling terkait, keterhubungan antar aplikasi dilakukan melalui interface-interface secara otomatis atapun manual *(batch*), ada beberapa aplikasi yang penting namun tidak terkait dengan bisnis proses utama perusahaan, yaitu seperti aplikasi-aplikasi CLM&LD, ECM dan EDW. Aplikasi-aplikasi tersebut tidak hanya melayani pengguna dari dalam seperti karyawan perusahaan dan aplikasinya, tapi juga melayani transaksi informasi dengan pengguna luar dan *network element* (NE). NE berada di sisi perangkat jaringan telekomunikasi, bahkan utamanya aplikasi-aplikasi tersebut digunakan untuk melayani pemrosesan data yang datang dari NE.

Diagram arsitektur aplikasi akan menggambarkan teknologi aplikasi yang sedang berjalan saat ini, terlihat betapa kompleknya keterhubungan antar aplikasi yang terpasang, sebenarnya aplikasi ini tersebar dalam satu area datacenter *(distributed system)* namun tetap terhubung satu sama lain, terjadinya gangguan pada salah satu sistem aplikasi tentunya bisa menggangu kinerja aplikasi-aplikasi yang lain. Kompleksifitas aplikasi-aplikasi ini menjadi tantangan yang menarik untuk menganalisa

arsitektur jaringan yang digunakan oleh aplikasi-aplikasi tersebut dan menyusun arsitektur teknologi dengan cara *reverse engineering* dilanjutkan dengan merancang arsitektur teknologi keamanan yang memadai dan sesuai untuk perusahaan. Gambar berikut ini menjelaskan arsitektur aplikasi perusahaan saat ini.




Gambar 3.1 Arsitektur Aplikasi

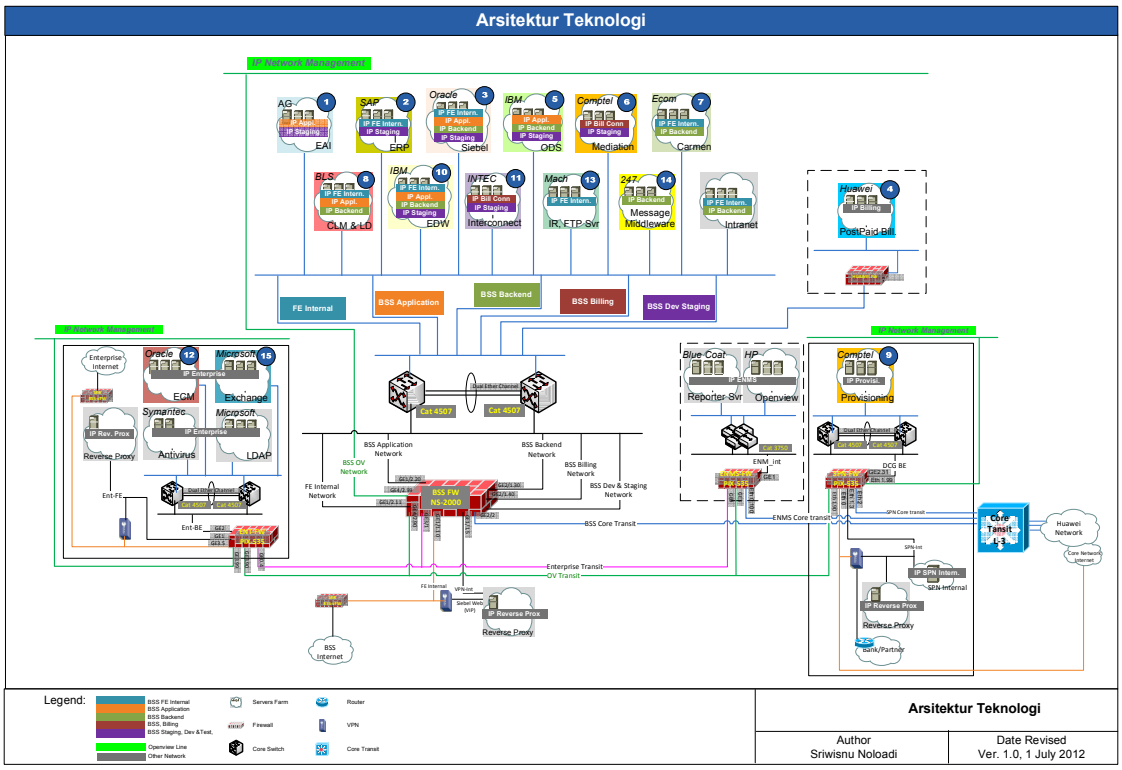
## 3.3 Arsitektur Teknologi Informasi Perusahaan

Perangkat teknologi informasi perusahaan berupa server menggunakan berbagai macam platform teknologi sistem operasi, seperti sistem operasinya menggunakan Windows Server, HP-UX, Redhat dan lain sebagainya, dari sisi teknologi database menggunakan berbagai macam sistem manajemen basis data seperti Oracle, DB2, MySQL, SQL Server dan lain sebagainya, selain itu penggunaan teknologi modern agar server beroperasi secara *realtime*, beberapa server telah mengadopsi teknologi *clustering* (*high availability and mirroring)*, teknologi ini berguna untuk menghindari berhentinya operasi server karena terjadinya *server crash* yang bisa mengakibatkan pengguna dan aplikasi tidak bisa mengakses server.

Selain itu hal yang sangat penting adalah bahwa hampir semua perangkat-perangkat server tidak memiliki perangkat software keamanan seperti anti virus, anti spam dan lain sebagainya, artinya banyak server-server tidak diinstall anti virus, anti spam atau perangkat lunak keamanan yang memadai baik itu pada server berbasis platform windows maupun yang berbasis platform unix dan linux. Untuk menjelaskan informasi tentang asset aplikasi dan hardware yang digunakan, tabel berikut ini merupakan data-data perangkat server di IT yang merupakan hasil analisa dan diolah menjadi satu tabel rangkuman yang merepresentasikan platform teknologi yang digunakan oleh aplikasi

Gambar berikut ini merupakan diagram overall arsitektur teknologi yang terdiri dari 14 aplikasi-aplikasi di BSS dan 1 aplikasi Exchange di

area ENT, yang mempunyai firewall masing-masing termasuk untuk area ENMS dan SPN.




Gambar 3.2 Arsitektur Teknologi

## 3.4 Perancangan Arsitektur Logis

### Manajemen Identitas

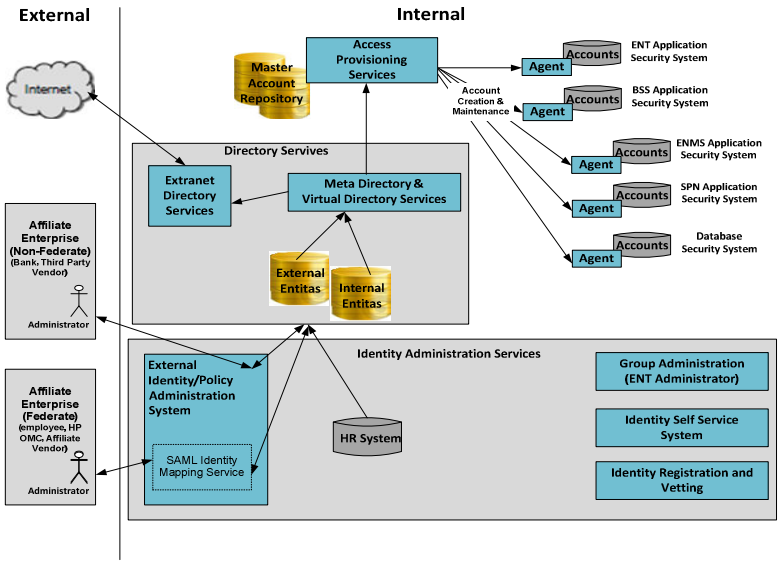
Arsitektur logis manajemen identitas *(IdM logical architecture)* harus menggambarkan layanan bagi pengaturan identitas secara logis, arsitektur ini harus menggambarkan layanan untuk melakukan proses administrasi identitas dari sisi internal dan eksternal, dan hubunganya dengan *directory services* serta layanan akses *provisioning* untuk mencapai suatu target berupa aset sumber daya IT yang dimiliki perusahaan. Gambaran mengenai arsitektur logis tentang manajemen identitas dibahas lebih banyak pada proses perancangan pada bab IV dan hasilnya harus disesuaikan dengan kondisi perusahaan dimana aset sumberdaya IT yang menjadi target eksekusi dipisahkan berdasarkan area-area security.

Secara lengkap layanan ini memberikan rincian tambahan berupa layanan IdM tertentu yang mungkin diperlukan, layanan ini bertanggung jawab untuk menetapkan dan mempertahankan identitas digital dan atribut terkait di lingkungan, termasuk proses menghapus dan mengatur identitas yang tidak valid dengan tujuan akuntabilitas.

Template layanan proses manajemen identitas dapat diuraikan sebagai berikut:

- Layanan administrasi user dan identitas
  - Layanan administrasi identitas
  - Layanan akses *provisioning (access rules and policies, account and privilege management)*
- Layanan direktori
  - Layanan direktori umum *(General purpose directory services)*
  - Layanan direktori khusus *(Special purpose directory services)*
  - Layanan direktori ekstranet *(Extranet directory services)*
  - *Meta directory* dan *virtual directory services*

Untuk menggambarkan arsitektur logis suatu *identity management* dapat digambarkan dalam gambar berikut ini.




Gambar 3.3 Arsitektur logis *Identity Management*

## 3.5 Perancangan Arsitektur Fisik Manajemen Identitas

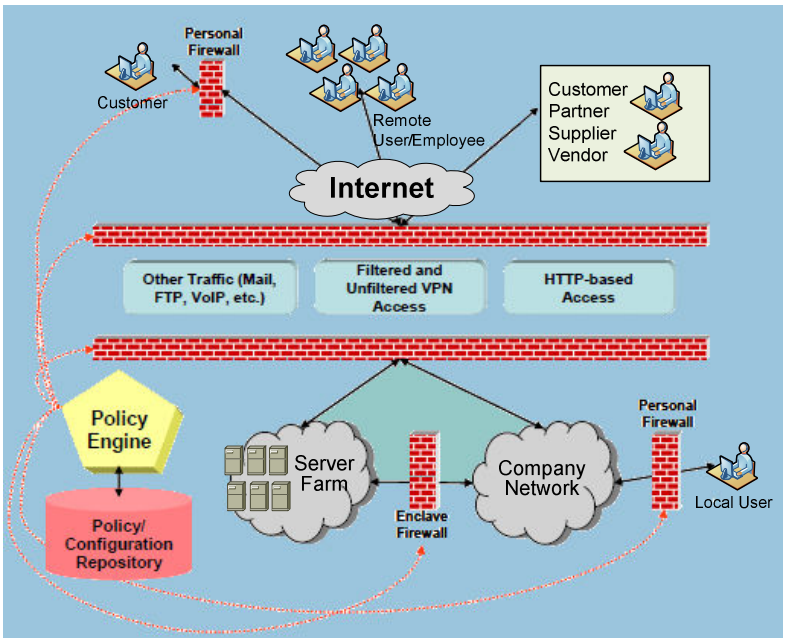
Arsitektur fisik manajemen identitas *(IdM physical architecture)* menggambarkan arsitektur yang akan diimplementasi secara fisik. Implementasi fisik suatu server, perangkat lunak, koneksi \jaringan, dan lain sebagainya dari lingkungan IdM yang dijabarkan dari arsitektur logis digambarkan secara kompleks. Untuk menggambarkan lingkungan seperti itu membutuhkan beberapa dokumen perusahaan terkait enterprise arsitektur, yaitu:

- Berbagai diagram seperti diagram komponen perangkat lunak pada server dan diagram topologi jaringan.
- Daftar alamat berbagai jaringan berupa alamat dari *Domain Controller* dalam suatu lingkungan manajemen identitas.
- Dokumentasi pengaturan konfigurasi untuk komponen perangkat lunak dan perangkat keras teknologi informasi.

## 3.6 Arsitektur Konseptual Border Protection

*Border protection services* bertanggung jawab untuk mengendalikan lalu lintas informasi yang melintasi batas batas eksternal atau internal antara zona keamanan, berdasarkan lokasi dari sumber lalu lintas dan tujuan atau pada isi lalu lintas secara fisik. Dalam model kebijakan ESA, banyak konfigurasi perangkat (termasuk pengguna akhir klien) menyediakan layanan perlindungan yang dikendalikan melalui kebijakan terpusat dengan definisi konfigurasi terhadap sumber daya *(resources)*.

Gambar berikut ini menujukan arsitektur konseptual *border protection* services, dimana setiap user baik itu customer, partner, suppl\ier, vendor ataupun karyawan yang melakukan proses remote login melalui jaringan internet dengan model vpn akan melalui beberapa pembatas berupa firewall bagian luar dan firewall bagian dalam.




Gambar 3.4 Arsitektur konseptual *border protection services*

## 3.7 Arsitektur Logis Border protection

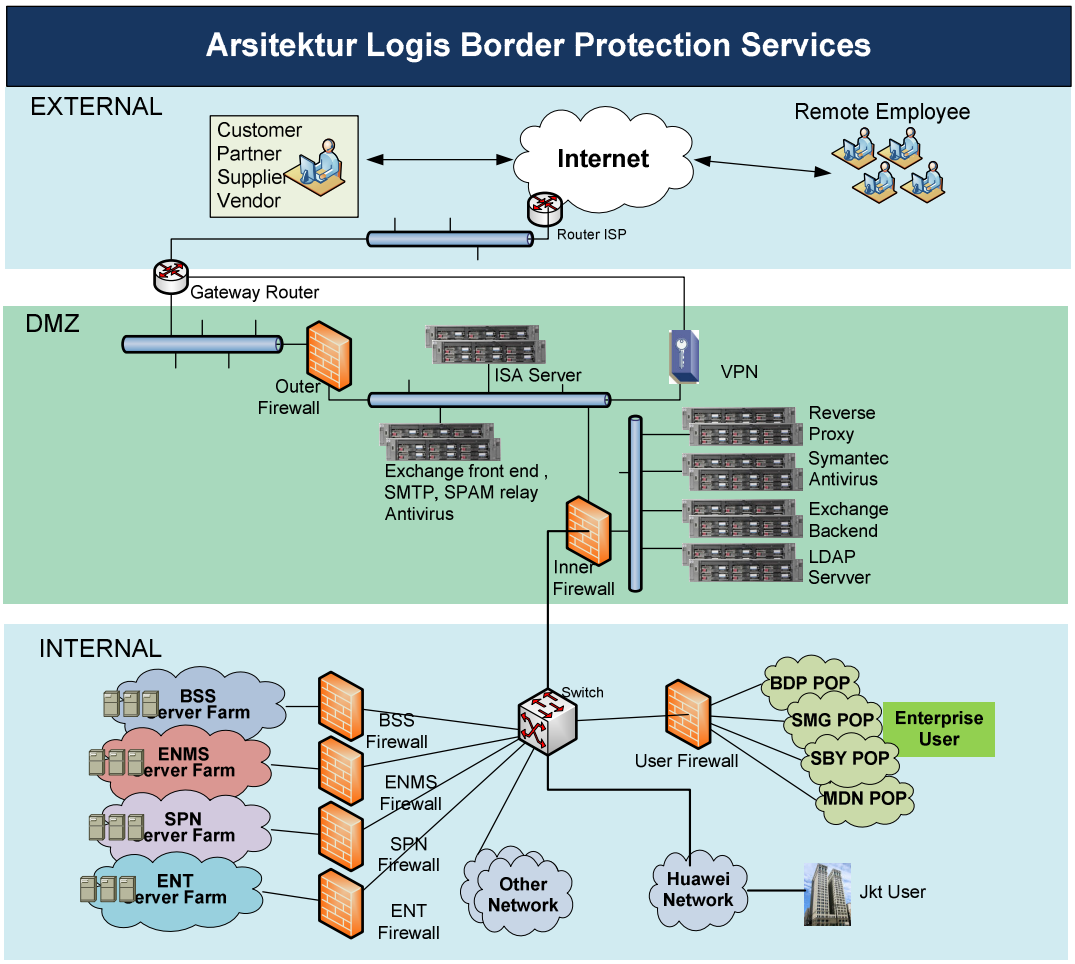
Dalam menyusun dan merancang *Security Technology Architecture* salah satunya adalah adalah menetapkan *border protection* yang mengedepankan arsitektur komunikasi yang lengkap berdasarkan high level, diagram topologi network saat ini, posisi router, switching dan firewall termasuk vpn devices, termasuk resources server farm di perusahaan. Setelah melakukan proses *reverse engineering* terhadap *high level* arsitektur jaringan teknologi informasi, *core transit connectivity*, *firewall security zoning* dan menganalisa hasil kajian teknologi yang digunakan saat ini termasuk diagram server-server farm, maka hasil dari proses ini dapat disusun suatu arsitektur logis *border protection* untuk perancangan *Security Technology Architecture* secara lengkap.

Berikut ini menjelaskan unsur-unsur utama dari arsitektur logis *border protection services*:

- Perangkat router mengelola internet routing dan menyediakan sarana penyaringan *packet filtering* berbasis IP/TCP/UDP protokol.
- Area *demilitarized zone* (DMZ) adalah segmen jaringan yang member fungsi terbatas untuk konektifitas antara *router gateway* dan *firewall* luar
- Firewall arah keluar harus mempunyai kinerja yang memamdai, yaitu:
  - Sebagai lapisan tambahan paket *filtering* IP/TCP/UDP.
  - Melakukan paket pemeriksaan dan pengecekan validitas protokol.
  - Mendeteksi dan mencegah kesalahan penolakan layanan atau *denial of service.*
  - Menjamin alamat IP routing digunakan untuk mengurangi kebocoran ruang alamat internet protokol.
- Segmen hosting DMZ adalah segmen jaringan antara *firewall* luar dan dalam yang mungkin berisi *host / server* berdasarkan kebutuhan yang diakses dari sisi luar dan sisi dalam.

Gambar berikut ini merepresentasikan arsitektur logis *border protection services* yang disesuaikan dengan kondisi di perusahaan, sangat jelas terlihat area external yang merupakan area tempat user melakukan login akses, area DMZ yang merupakan area konektifitas antara external

dan internal serta area internal yang merupakan lingkungan *resources server farms* ditempatkan.




Gambar 3.5 Arsitektur logis *border protection services*

## 3.8 Rancangan Arsitektur Fisik Terkait Infrastruktur Perusahaan

Diagram arsitektur secara fisik yang lengkap harus menggambarkan zoning keamanan IT dan semua perangkat jaringan diluar lingkungan dan didalam IT yang saling berhubungan yang merepresentasikan rancangan yang baku yang disesuaikan dengan arsitektur jaringan teknologi informasi di perusahaan, melalui proses yang cukup panjang akhirnya bisa diidentifikasi semua perangkat jaringan dan keamanan diperusahaan berdasarkan nama *host* pada semua perangkat yang terhubung, nama host-nama host tersebut berhasil diidentifikasi berdasarkan referensi yang diambil dari data inventaris perangkat router, switch, firewall dan lain sebagainya, sebagai contoh jaringan yang menghubungan perangkat-perangkat di kota Bandung ke dalam lingkungan data center perusahaan melalui perangkat-perangkat komunikasi sebagai berikut: dari sisi Bandung User terhubung ke perangkat router BDG01-POP-R1/BDG01-POP-R2, perangkat ini terhubung dengan router di Jakarta melalui jaringan POP kedalam perangkat router CIG01-CORE-BDR1/CIG01-CORE-BDRF2 dan dirouting melalui router CIG01-POP-R1/CIG01-POP-R2 untuk akses masuk kedalam *network internal* di *data center*.

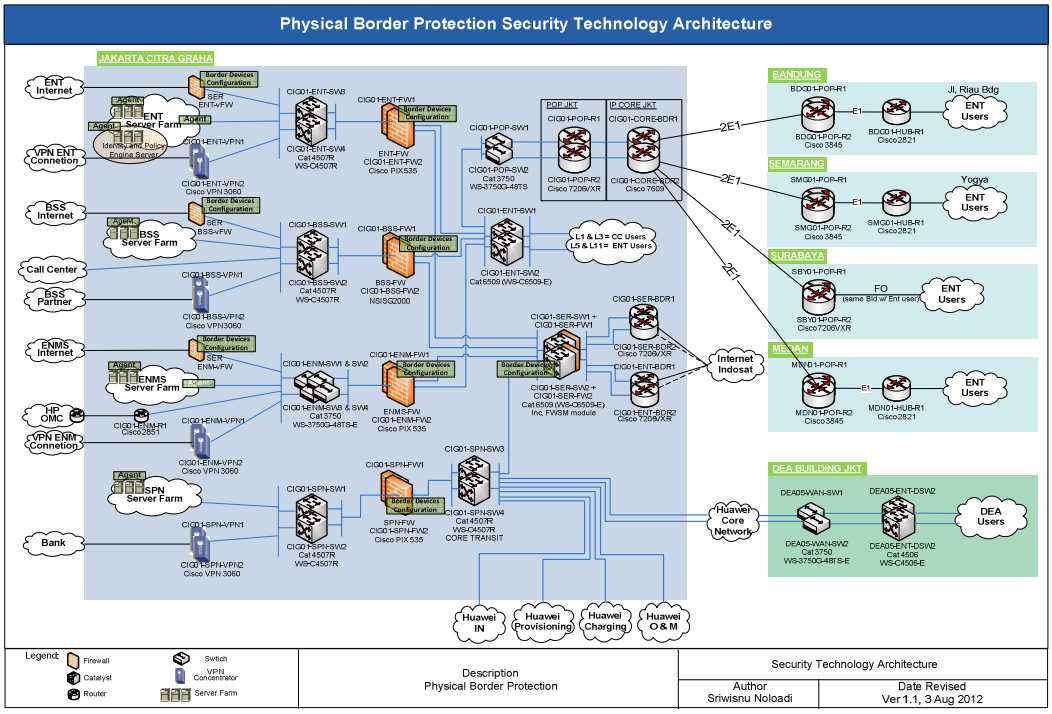
Diluar jaringan POP antar kota ada jaringan fiber optik yang menghubungkan antara menara DEA (area user) dan *data center*, koneksinya dihubungkan dengan *core network* Huawei *fiber optic*, selain itu diagram jaringan ini

juga menggambarkan sisi external jaringan yaitu yang terhubung dengan koneksi internet termasuk *virtual private network* (VPN) untuk fasilitas remote access yang disediakan bagi karyawan dan pihak ketiga seperti afilasi vendor dan lain sebagainya.

Dalam kaitannya dengan *Security Technology Architecture*, IdM dan *policy driven* diterapkan pada arsitektur tersebut yang bertujuan sebagai pengatur semua kebijakan dan *enforcement* terhadap resources-resources melalui services yang disediakan, setiap perangkat jaringan keamanan akan memiliki format kebijakan yang ditempatkan, mungkin dalam bentuk XML yang diinjeksi kedalam sistem konfigurasi perangkat keamanan, lalu dibutuhkan *agent-agent* yang bisa saja dipasang pada perangkat teknologi seperti *server, storage system, perangkat router* dan *switch* sehingga melengkapi konsep penerapan dari *Security Technology Architecture*, agent inilah yang akan mengecek apakah permintaan yang dikirim oleh pengguna *user* dan aplikasi sesuai dengan kebijakan yang diterapkan, mulai dari kecocokan identitas pengguna dan aturan *(role)* yang ditetapkan oleh PDP engine.

Diagram arsitektur yang lengkap tentang *Security Technology Architecture* terkait infrastruktur perusahaan dirancang sesuai termasuk *overall* arsitektur jaringan perusahaan, termasuk *firewall* sesuai dengan konfigurasi pada *border protection* untuk teknologi keamanan yang diinginkan berdasarkan konsep *Security Technology Arcitecture* yang menerapkan IdM dan PD. Sesuai dengan pemahaman tentang teknologi arsitektur maka secara efesien perangkat server bisa memasang *agent-agent* yang bisa mengijinkan proses *policy enforcement* terhadap resources, jadi secara fisik dan efisien perusahaan hanya cukup menambahkan server-server IdM dan *Policy Engine* di area ENT untuk menerapkan *Security Technology* yang diharapkan.

Gambar berikut ini merupakan rancangan *Security Technology Architekture* terkait infrastruktur perusahaan, rancangan ini menjelaskan server *IdM* dan *Policy Engine* server yang bisa diimplementasi diperusahaan untuk menjalankan *Security Technology,* semua layanan PMA *(Policy Management Access)* dan *Security Services* termuat didalam layanan server-server tersebut.




Gambar 3.6 Diagram fisik *Security Technology Architecture* pada jaringan perusahaan

Untuk melengkapi penelitian ini, akan diuraikan kapabilitas *Policy Management Access* (PMA) dan *security services* dalami *Security Technology Architecture* yang dirancang, berdasarkan literatur yang dipelajari dan dianalisa terhadap kondisi perusahaan saat ini, tabel berikut ini akan merepresentasikan dan menjelaskan kapabilitas yang dimiliki perusahaan setelah menerapkan *Security Technology Architecture,* kapabilitas-kapabilitas tersebut nantinya harus bisa diuji dengan melibatkan kontrol yang terkait dengan layanan tersebut, untuk itu perlu disusun dan diuraikan deskripsi kemampuan apa saja yang bisa dilakukan oleh PMA yang melakukan fungsi provisioning dan *security services* yang melakukan layanan keamanan sesuai dengan penerapan *Security Technology Architecture* yang dirancang.

Tabel 3.2 Kapabilitas layanan provisioning secara fungsional

| ***Policy Management & Security Services*** | ***Category Services*** | ***Capabilities*** | ***Control*** | ***Category Control*** |
|---|---|---|---|---|
| ***Provisioning Functionality*** | ***Identity Management*** | Pengaturan identitas | *Identification, Security Administration* | *Supporting Technical Control* |
| | ***Access Management Services*** | Pengaturan akses | *Access Control* | *Supporting Technical Control* |
| | ***Configuration Mgm Services*** | Pengaturan konfigurasi sistem | *Audit, Restore Secure State* | *Detection & Recovery Control* |

Tabel 3.3 Kapabilitas layanan security secara fungsional

| *Policy Management & Security Services* | *Category Services* | *Capabilities* | *Control* | *Category Control* |
|---|---|---|---|---|
| **Security Services** | ***Access Control Services*** | | | |
| | *Authentication (Direct & Indirect)* | Memverifikasi account<br>Mengotentikasi password, token | *Authentication Control* | *Preventive Control* |
| | *Authorization (Online & Offline)* | Memberikan otorisasi akses kepada pengguna sah | *Authorization Control* | *Preventive Control* |
| | ***Border Protection Services*** | Layanan pembatasan akses secara fisik | *Protected Communication* | *Preventive Control* |
| | ***Detection Services*** | | | |
| | *Intrusion* | Mendeteksi gangguan<br>Mengendalikan gangguan | *Intrusion and Containtment* | Detection & Recovery Technical Control |
| | *Anomaly* | Mengidentifikasi penyimpangan | *Anomaly Control* | Detection & Recovery Technical Control |
| | *Vulnerability assessment* | Menilai kerentaan keamanan | *Assessment Control* | Detection & Recovery Technical Control |
| | *Logging Services* | Mencatat & mengumpulkan log<br>Mengkonsolidasi log | *Log Control* | Detection & Recovery Technical Control |
| | ***Content Control Services*** | | | |
| | *Anti-Virus* | Mendeteksi virus<br>Menberantas virus | *Virus Detection and Eradication* | Detection & Recovery Technical Control |
| | *Anti-Spam* | Mendeteksi spam<br>Menyaring spam | *Spam Detection and Filtering* | *Detection & Recovery Technical Control* |
| | *Ent. Right Mgm Services* | Melindungi dokumen *digital* | *Protection Control* | *Management Security Control* |
| | *Content Inspection* | Menginspeksi isi informasi digital | *Content Control* | *Preventive Control* |
| | ***Auditing Services*** | Memastikan integritas<br>Menyelidiki insident<br>Memastikan kesuaian kebijakan<br>Memantau pengguna dan aktivitas | *Audit Control* | *Detection & Recovery Technical Control* |
| | ***Cryptographic Services*** | | | |
| | *Cryptography Services* | Melakukan enkripsi<br>Melakukan dekripsi | *Cryptography Key Management* | *Supporting Technical Control* |
| | *Public Key Infrastructure* | Melakukan sertifikasi otorisasi proses | *Public Key Management* | *Supporting Technical Control* |
| | *Private Key Storage* | Menyimpan private key<br>Menjaga kerahasian informasi | *Private Key Management* | *Supporting Technical Control* |
| | *Digital Signature Services* | *Signing Service*<br>*Notary Services*<br>*Code Signing Services*<br>*Verification Services* | *Digital Signature Management* | *Supporting Technical Control* |

## 4. Kesimpulan dan Saran

Dari hasil penelitian tentang *Security Technology Architecture,* dapat ditarik kesimpulan-kesimpulan sebagai berikut:

1. Penelitian *Security Tehcnology Architecture* bagi PT "N" merupakan studi tentang penyusunan arsitektur teknologi keamanan yang memadai untuk perusahaan
2. Walaupun dirasa sangat penting karena tingkat kesulitan yang tinggi akan pengetahuan tentang keamanan, PT "N" belum menerapkan teknologi keamanan berbasis kebijakan.
3. Menyusun dan merancang *Security Technology Architecture* untuk PT "N"

menggunakan *framework Enterprise Security Architecture* (ESA) dari *Network Applications Consortium* (NAC) yang sekarang telah bergabung dengan Open Group..

4. Dalam meningkatkan kualitas perancangan teknologi keamanan yang memadai di PT "N" diperlukan analisa yang matang tentang enterprise arsitektur teknologi informasi saat ini, menyusun profil risiko perusahaan, menyimpulkan kontrol validasi terhadap gap analysis untuk melakukan penilaian risiko.
5. Untuk memitigasi risiko teknologi infromasi terkait keamanan PT "N" dapat penyusunan dan perancangan *Security Technology Architecture* berdasarkan *framework* ESA dari OpenGroup yang melalui 4 (empat) tahapan penting yaitu: menyusun dan merancang kerangka kerja konseptual, menyusun kerangka kerja arsitektur konseptual, merancang arsitektur logis dan merancang arsitektur fisik.

Adapun saran yang dapat diuraikan dari hasil penelitian ini adalah sebagai berikut:

1. Observarsi yang dilakukan untuk menyusun dan merancang *Security Technology Architecture* di PT "N" harus dilakukan secara mendalam karena kompleksifitas sistem informasi di perusahaan.
2. Untuk membantu proses perancangan *Security Technology Architecture* di PT "N" disarankan menggunakan *framework-framework* tambahan untuk menganalisa sistem yang sedang berjalan, menyusun profil risiko dan menyusun kontrol validasi terhadap *gap analysis* sebagai acuan pentingnya rancangan teknologi keamanan ini
3. Sebaiknya PT "N" segara menerapkan *Security Technology Architecture* untuk memitigasi risiko teknologi informasi perusahaan.

## 5. Daftar Pustaka


1. Obeid, Doug., 2003 - 2004, NAC-Network Applications Consorsium: *"Enterprise Security Architecture"* Journal of NAC, E-Journal on-line. Trough http://trygstad.rice.iit.edu:8000/Articles/EnterpriseSecurityArchitecture-NetworkApplicationsConsortium.pdf [June 1, 2012, 6:40pm]
2. Gary Stoneburner, Alice Goguen, and Alexis Feringa, 2002, NIST sp800-30: *"Risk Management Guide for Information Technology Systems"* Journal of NIST. E-Journal on-line. Trough http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf [July 19, 2012, 7.40pm]
3. NIST Special Publication 800-53 Revision 3, 2009, NIST sp800-53: *"Information Security"* Journal of NIST. E-Journal on-line. Trough http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf., [July 20, 2012, 2.26pm]
4. Henk Jonkers (Ed.), Iver Band, Dick Quartel, Henry Franken, Mick Adams, Peter Haviland, and Erik Proper., July 2012. "*Using The TOGAF 9.1 Architecture Content Framework with the Archimate 2.0 Modeling Language"*. Journal of Opengroup. E-Journal on-line. Trough https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?publicationid=12697 [July 18, 2012, 6.34am]
5. De Haes, Steven, Ph.D. du Preez, Gert, CGEIT. Massa, Rachel, CGEIT. Bart,

Peeter. Steve, Reznik, CISA. Steuperaert, Dirk, CISA, CGEI, 2009. *"The Risk IT Practioner Guide"*