BAB III

PEMBAHASAN

3.1 Jadwal Kerja Praktek

Pelaksanaan kerja praktek dilaksanakan di PT. Telekomunikasi, Tbk (TELKOM) Indonesia, di Jl. Japati No. 1 Lantai 4 Bandung. Adapun pelaksanaa kerja praktek dimulai pada tanggal 18 Juli 2010 sampai dengan tanggal 18 Agustus 2010.

3.2 Data Kerja Praktek

Data kerja yang dimaksud adalah segala sesuatu yang berhubungan dengan referensi yang mendukung kegiatan monitoring *Security Email Gateway* yang ada di PT. Telekomunikasi (Telkom) Divisi ISC, adapun tool yang digunakan untuk mendukung Kerja Praktek ini adalah IronPort C360 dalam memonitoring setiap *email* yang keluar atau masuk agar meminimalisir kemungkinan serangan *virus* atau *spam* yang dapat mengancam keamanan System atau keamanan Data Perusahaan.

3.2.1 Pengertian Monitoring, Security Email Gateway

Monitoring adalah proses pengumpulan data dan pengukuran atas objektifitas program atau memantau perubahan yang fokus pada proses dan

keluaran. Monitoring melibatkan perhitungan atas apa yang kita lakukan dan melibatkan penggamatan atas kualitas dari apa yang kita kerjakan.

Keamanan data di surat elektronik tidaklah terjamin dan selalu ada risiko terbuka untuk umum, dalam artian semua isinya dapat dibaca oleh orang lain. Hal ini disebabkan oleh karena surat elektronik itu akan melewati banyak *server* sebelum sampai di tujuan. Tidak tertutup kemungkinan ada orang yang menyadap surat elektronik yang dikirimkan tersebut.

Surat elektronik dapat diamankan dengan melakukan teknik pengacakan (enkripsi). Salah satu program enkripsi yang populer adalah PGP (*Pretty Good Privacy*). Dengan memakai PGP maka isi akan dienkrip, dan hanya orang yang tertuju dapat mendekripsi dan membaca surat elektronik tersebut. Kerugiannya adalah membuat repot pihak pengirim dan penerima (karena keduanya harus memiliki program PGP, dan pengirim juga harus memiliki kunci umum penerima, dan melakukan enkripsi pesan dengan kunci tersebut).

Gateway adalah sebuah perangkat yang digunakan untuk menghubungkan satu jaringan komputer dengan satu atau lebih jaringan komputer yang menggunakan protokol komunikasi yang berbeda sehingga informasi dari satu jaringan computer dapat diberikan kepada jaringan komputer lain yang protokolnya berbeda. Definisi tersebut adalah definisi gateway yang utama.

3.2.2 Sekilas Perangkat Cisco IronPort C360

IronPort system adalah sebuah unit usaha Cisco yang menyediakan peralatan anti-spam, anti-virus, dan ati-spyware untuk organisasi mulai dari usaha kecil ke Global 2000. IronPort memanfaatkan peralatan SenderBase email terbesar di dunia dan jaringan deteksi ancaman web dan DataBase.

Skala dan kompleksitas serangan *virus-virus* baru ini telah menyoroti pentingnya platform, pesan yang kuat dan aman untuk melindungi parimeter jaringan anda. Untuk memerangi ancaman ini berkembang, beberapa solusi dari IronPort yaitu *multi-scan, multi-vendor* :

- Lapisan pertama yan merupakan pertahanan pencegahan terhadap Wabah *virus* baru.
- Mengintegrasikan Mcafee dan Sophos *anti-virus* engine yang memunkinkan beberapa metode pendektesian virus untuk memastikan perlindungan terhadap serangan virus yang paling kompleks.



Gambar 3.1 IronPort Teknologi Proprietary

3.2.3 Cisco IronPort anti-Spam

Lapisan pertama dari kontrol *spam,* digunakan untuk mengklasifikasikan pengiriman *email* dan membatasi akses ke *email*

infrastruktur berdasarkan pengirim. Lapisan kedua melakukan pertahanan, pemindaian. Pesan dari pengirim yang tidak dikenal atau kurang terpercaya dapat dikenakan pemindaian *anti-spam* dan anda bisa menolak sejumlah pesan yang diterima dari setiap pengirim.

- Pemindaian :

Work Queue	Message Filters *	
	Safelist/Blocklist Scanning	
	Anti-Spam **	Per Recipient Scanning
	Anti-Virus **	
	Content Filters *	
	Virus Outbreak Filters *	

Tabel 3.1 Pemindaian IronPort

- Message Filter diterapkan sebelum pesan * Dapat mengirim pesan ke karantina "pecah.".
- AsyncOS memeriksa alamat pengirim dengan database pengguna akhir safelist / blocklist. Jika alamat pengirim safelisted, anti-spam pemindaian akan dilewati. Pesan dapat pecah jika ada beberapa penerima. * Dapat mengirim pesan ke karantina jika pengirim blocklisted.
- Anti-Spam memeriksa mesin pemindaian pesan dan mengembalikan putusan untuk diproses lebih lanjut.

- Anti-Virus scanning memeriksa pesan untuk virus. Pesan-scan dan opsional diperbaiki, jika mungkin. * Dapat mengirim pesan ke karantina.
- Content Filter diterapkan. DKIM, SPF, dan verifikasi SIDF dilakukan jika kondisi filter konten yang sesuai didefinisikan. * Dapat mengirim pesan ke karantina.
- Virus Outbreak Filter fitur membantu melindungi terhadap wabah virus. * Dapat mengirim pesan ke karantina. Gateway virtual Mengirim email melalui antarmuka IP tertentu atau kelompok antarmuka IP.

- Pertahanan :

User dapat menggunakan halaman ini untuk memantau pertahanan melawan serangan virus. Bagian Status Sekarang menyediakan informasi tentang konfigurasi Data wabah global secara otomatis download dari IronPort Threat Center Operasi satu jam sekali. Perhatikan bahwa alat IronPort harus mampu berkomunikasi.

Ringkasan daftar Wabah virus global serta wabah virus lokal, yang memungkinkan *user* untuk membandingkan tren virus jaringan lokal untuk tren global. Data wabah virus global mewakili semua wabah yang terdeteksi oleh IronPort Threat Center Operasi yang melebihi ambang batas saat ini dikonfigurasi untuk di karantina. Data wabah

virus lokal mewakili semua wabah terdeteksi pada IronPort Threat Center Operasi yang melebihi ambang batas saat ini dikonfigurasi untuk wabah karantina. Rata-rata Waktu Perlindungan selalu didasarkan pada perbedaan ketika setiap ancaman terdeteksi oleh IronPort Threat Center Operasi dan pelepasan tanda anti-virus oleh vendor besar.

Perhatikan bahwa tidak setiap wabah virus global mempengaruhi alat IronPort. Hal ini tidak menunjukkan waktu perlindungan nol, melainkan berarti bahwa informasi yang diperlukan untuk menghitung waktu perlindungan tidak tersedia. Bagian Pesan Dikarantina Wabah Virus dan merupakan ukuran yang potensial untuk menghitung jumlah pesan yang dianggap sebagai ancaman. Pesan yang dikarantina dihitung pada saat rilis. Biasanya, pesan akan dikarantina sebelum anti-virus tersedia. Ketika dirilis, virus akan dipindai dengan perangkat lunak anti-virus untuk menjadi virus positif atau bersih. Jika anti-virus software tidak diaktifkan pada alat IronPort, jumlah pesan virus terdeteksi positif akan selalu menjadi nol.

Karena sifat dinamis dari pelacakan Virus Wabah, aturan di mana pesan dikarantina (dan bahkan wabah yang terkait) dapat berubah sewaktu pesan di karantina. Menghitung pesan pada saat rilis (daripada saat masuk ke dalam karantina) menghindari kebingungan memiliki jumlah yang meningkatkan dan menurunkan. Para Wabah Rincian daftar menampilkan informasi tentang wabah yang spesifik, termasuk

ID, waktu dan tanggal wabah itu pertama kali terlihat secara global, lead time yang disediakan oleh filter Wabah Virus, dan jumlah pesan dikarantina. Anda dapat memilih wabah baik global atau lokal serta jumlah pesan untuk menampilkan melalui menu di sebelah kiri. Anda dapat mengurutkan daftar dengan mengklik header kolom.

Pertama Dilihat global waktu ditentukan oleh IronPort Threat Center Operasi, berdasarkan data dari SenderBase, email terbesar di dunia dan web lalu lintas jaringan pemantauan. Para Wabah Virus Filter time Perlindungan didasarkan pada perbedaan antara ketika setiap ancaman terdeteksi oleh IronPort Threat Center Operasi dan pelepasan tanda tangan anti-virus oleh vendor besar. Nilai "-" menunjukkan baik perlindungan waktu tidak ada, atau waktu tanda tangan tidak tersedia dari anti-virus vendor (beberapa vendor tidak dapat melaporkan kali tanda tangan). Hal ini tidak menunjukkan waktu perlindungan nol. Sebaliknya, itu berarti bahwa informasi yang diperlukan untuk menghitung waktu perlindungan tidak tersedia.

Menggunakan halaman Wabah Virus, Anda dapat menjawab pertanyaan seperti:

- Berapa banyak pesan yang sedang dikarantina dan yang Wabah Virus aturan Filter?
- Berapa banyak waktu telah menyebabkan Filter Virus Wabah fitur telah menyediakan untuk virus wabah?

- Bagaimana wabah virus lokal saya dibandingkan dengan wabah global?

Anda tidak dapat mengkonfigurasi urutan virus scanning. Ketika Anda mengaktifkan multi-lapisan anti virus scanning, scan engine McAfee virus pertama, dan scan mesin Sophos virus kedua. Jika mesin McAfee menentukan bahwa pesan yang bebas virus, mesin scan Sophos pesan, menambahkan perlindungan lapis kedua. Jika mesin McAfee menentukan bahwa pesan berisi virus, IronPort alat scanning dan melompat Sophos melakukan tindakan pada pesan virus berdasarkan pengaturan yang Anda dikonfigurasi.

3.2.4 Cisco IronPort anti-Virus

Alat IronPort Anda termasuk mesin pemindaian virus terintegrasi. Anda dapat mengkonfigurasi alat untuk memindai pesan dan lampiran untuk virus pada per-dasar "surat kebijakan". Anda dapat mengkonfigurasi alat untuk melakukan hal berikut ketika virus ditemukan:

• berusaha untuk memperbaiki lampiran

• penurunan lampiran

• memodifikasi header subjek

• menambahkan header-X tambahan

• mengirim pesan ke alamat yang berbeda atau mailhost

• arsip pesan

• menghapus pesan

Pesan dilepaskan dari karantina di-scan untuk virus.

3.2.5 Bounced Mail

Sebuah bouncing yang terjadi karena pesan yang dikembalikan setelah pesan itu diterima untuk pengiriman oleh host penerima. Ini dapat menjadi soft atau hard bouncing. Anda dapat menganalisis tanggapan-tanggapan bouncing untuk menentukan apa yang harus dilakukan dengan penerima pesan (misalnya mengirim ulang pesan soft bounced penerima dan menghapus hard bounced penerima dari database).

- Hard Bounced

  Sebuah pesan yang tidak terkirim secara permanen. Hal ini dapat terjadi selama percakapan SMTP atau sesudahnya.

- Soft Bounced

  Sebuah pesan yang pengiriman akan menyerang kembali pada basis waktu yang akan dikonfigurasi pelacakan maksimum atau waktu maksimum dalam antrian.

3.2.6 Email Security

Peralatan keamanan IronPort *email* memberikan pendekatan multi-lapisan untuk menghentikan *email* berbasis ancaman :

a. Untuk perlindungan *spam, email.*

b. Filter *outbrake virus* Cisco IronPort dipasangkan dengan terintegrasi teknologi *anti-virus* tradisional untuk mengaktifkan pertahanan *virus* paling kuat. IronPort mengintegrasikan keinfrastrukturan pesan yang ada, memberikan pertahanan kemanan mendalam.



Gambar 3.2 Infrastruktur Keamanan Email

3.2.7 Encryption DataSheet

Untuk mengkonfiurasi enskripsi email outbond pada tool keamanan *email,* ikuti langkah-langkah berikut :

1. Jika anda ingin menggunakan *server* kunci lokal, mengkonfiurasi tool enskripsi IronPort.

2. Konfigurasikan profil enkripsi, untuk mengaktifkan *enskripsi email*, ikuti langkah-langkah berikut :

a. Klik Keamanan > enskripsi email IronPort

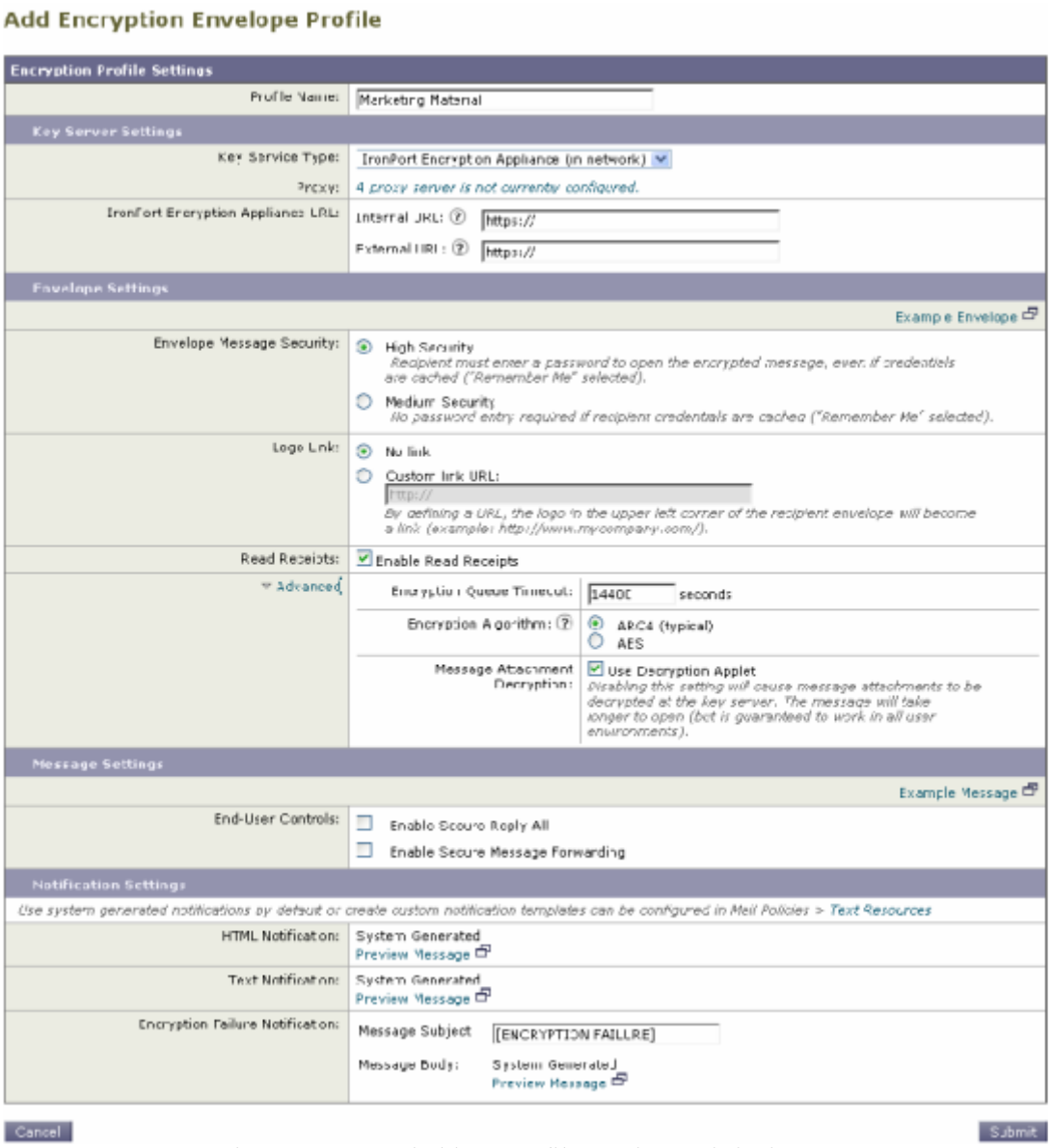
b. Klik aktifkan

c. Opsional, klik Edit pengaturan dan mengkonfigurasi *server proxy.*



Gambar 3.3 Konfigurasi Global Setting

3. Jika ingin mengunakan layanan kunci *host,* membuat layanan amplop akun Cisco terdaftar.anda membuat akun dengan cara mengklik tombol penyediaan setelah mengkonfigurasi profile enskripsi.



Gambar 3.4 Menambahkan Profil Amplop Enkripsi

4. Mengkonfigurasi filter konten keluar, anda perlu mengkonfigurasi filter konten untuk menandai email outbond yang harus di enkripsi. Untuk membuat filter konten enkripsi :

a. Klik Mail Policies > Outgoing Content Filters.

b. Pada bagian Filter, klik Add Filter.

c. Pada bagian Conditions section, klick Add Condition.

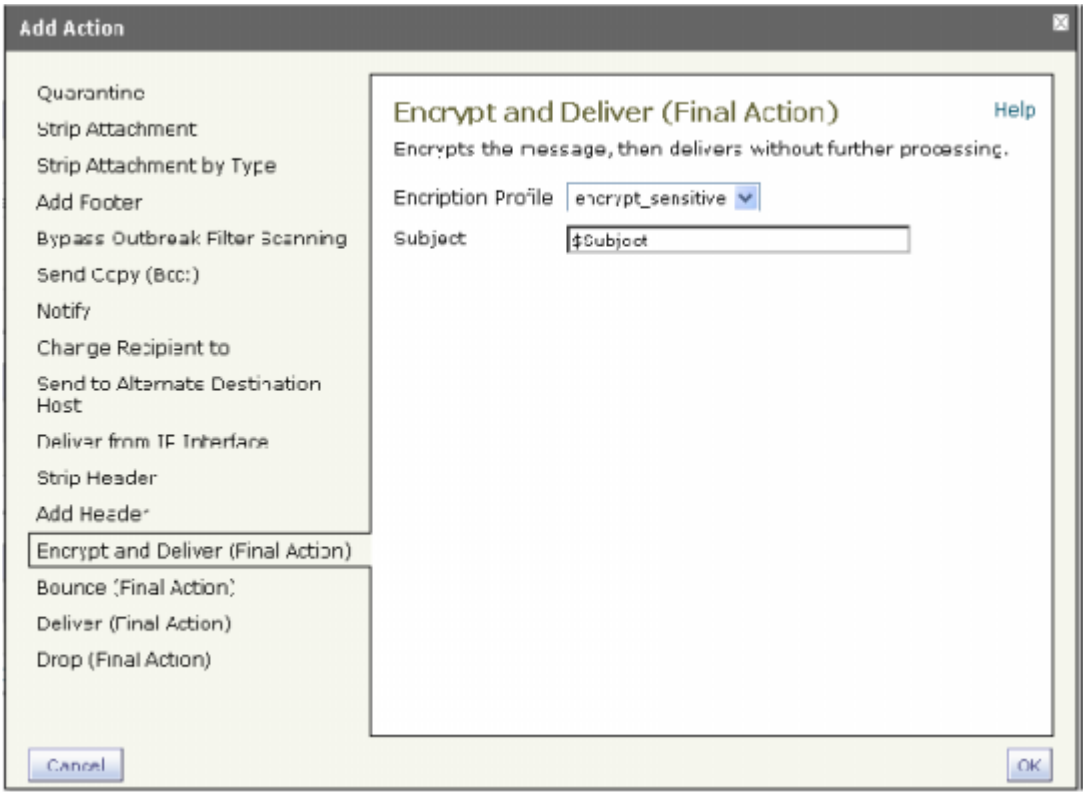
d. Tambahkan kondisi untuk menyaring pesan yan ingin anda enkripsi, misalnya untuk mengenkripsi bahan yang sensitif, anda bisa menambahkan kondisi yan berisi kata tertentu, contohnya “Rahasia” dalam subjek.

e. Klik OK.

f. Opsional, klik Add Action dan pilih Add Header untuk memasukkan header enkripsi ke pesan untuk meenentukan pengaturan enkripsi tambahan.

g. Pada bagian Actions, klik Tambah Aksi.

h. Pilih Encrypt dan Deliver.



Gambar 3.5 Konfigurasi Mengenkripsi dan Memberikan Aksi

Web browser yang support :

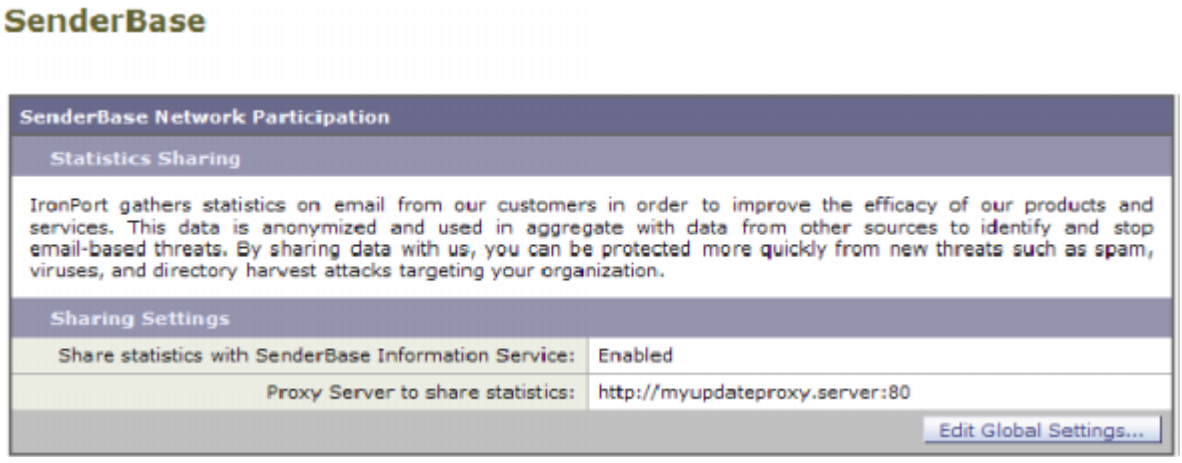
1. Microsoft Internet Exploler 6
2. Microsoft Internet Exploler 7
3. FireFox 2.0
4. FireFox 3.0

3.2.8 SenderBase Overview

SenderBase adalah layanan reputasi *email* yang dirancang untuk membantu *Administrator email* meneliti pengirim *email,* menidentifikasi sumber-sumber yang sah dari *email,* dan *spammer* blok. Dalam pengaturan sistem wizard (GUI) dan perintah system setup (CLI), anda dapat setuju untuk berpartisipasi dalam jaringan SenderBase.

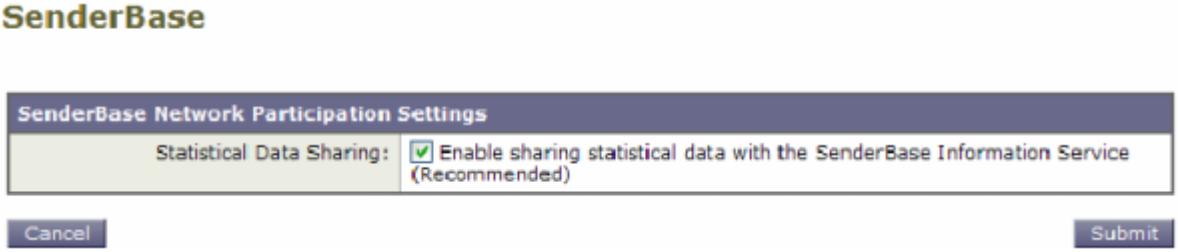
IronPort akan mengumpulkan statistiik *traffic agregat email* tentang organisasi anda. Ini termasuk ringkasan data hanya pada atribut pesan dan informasi tentang bagaimana berbagai jenis pesan ditangani oleh tool IronPort. Misalnya, IronPort tidak mengumpulkan pesan atau subyek pesan, informasi pribadi atau informasi yang mengidentifikasikan organisasi anda akan dirahasiakan. Untuk berbagi statistik dari IronPort dengan jaringan SenderBase :

1. Akses Security Service > SenderBase page.



Gambar 3.6 SenderBase Page

2. Klik edit Global Setting



Gambar 3.7 Setting SenderBase

3. Tandai kotak untuk mengaktifkan berbagai data statistik dengan layanan informasi SenderBase. Mencentang kotak ini untuk enable fitur tool global.
4. Sebagai pilihan, anda dapat mengaktifkan *server proxy* intuk bagi data statistik dengan layanan informasi SenderBase. Anda dapat mengkonfigurasi pengaturan yang sama dengan menggunakan perintah senderbaseconfig pada CLI.

3.2.9 Virus DataSheet

Skala dan kompleksitas serangan virus baru-baru ini telah menyoroti pentingnya platform, pesan kuat yang aman untuk melindungi perimeter jaringan Anda. Pendekatan tradisional yang mampu mengidentifikasi dan memblokir virus yang dikenal tidak lagi cukup. Untuk memerangi ancaman ini berkembang, IronPort ® menawarkan solusi multi-scan, multi-vendor anti-virus yang paling komprehensif:

1. Filter Wabah Virus IronPort ™ - lapisan pertama yang kritis pertahanan pencegahan terhadap wabah baru, mendeteksi dan menghentikan virus sebelum teknologi lainnya.
2. McAfee yang terpadu dan Sophos anti-virus engine - memungkinkan beberapa metode pendeteksian virus tradisional untuk memastikan perlindungan terhadap serangan virus bahkan yang paling kompleks.

Fitur Virus datasheet :

1. Pencegahan dan Perlindungan Wabah Virus.

Selama wabah virus apapun, selalu ada periode waktu antara deteksi virus dan ketika file anti-virus identitas yang sebenarnya disebarkan. Selama periode ini, administrator dapat memanfaatkan teknologi Filter Wabah Virus IronPort untuk mengidentifikasi dan virus karantina berdasarkan pola yang dikenal dan menghapus atau mengarsip pesan sampai file identitas baru dapat diperbarui.

2. Metode Deteksi Ganda (perlindungan terhadap berbaai pengembangan virus).

Selama proses scanning, McAfee dan Sophos anti-virus engine baik menganalisis setiap pesan yang masuk dan file, mengidentifikasi jenis dan kemudian menerapkan teknik yang relevan

untuk memastikan keberhasilan tertinggi dan throughput. McAfee dan Sophos anti-virus engine menggunakan metode deteksi ganda, seperti:

a. **Pencocokan Pola** mendeteksi virus dan software yang mungkin tidak diinginkan lainnya dengan urutan kode tertentu yang diketahui dalam virus. Pola ini diciptakan untuk memastikan bahwa mesin tidak hanya menangkap virus asli tapi derivatif dalam keluarga virus yang sama. Dengan demikian, McAfee dan Sophos mendekatan virus dalam mode komplementer. Mesin pemindaian McAfee dimulai dari sebuah tempat yang dikenal dalam sebuah file, kemudian mencari virus signature. Sering kali, mereka harus mencari hanya sebagian kecil dari file untuk menentukan bahwa file ini bebas dari virus. Sebaliknya, mesin pemindaian Sophos mencari beberapa urutan kode pendek bersamaan untuk mendeteksi virus signature.
b. **Teknologi canggih emulasi** digunakan untuk mendeteksi virus yang dienkripsi dan polymorphic. Jika mesin mencurigai bahwa sebuah file berisi virus, menciptakan sebuah lingkungan buatan di mana virus dapat berjalan tanpa membahayakan sampai decode itu sendiri dan bentuk sebenarnya menjadi terlihat. Mesin kemudian mengidentifikasi virus dengan memindai virus. Mesin yang kuat mendukung mode pemindaian ganda untuk mengoptimalkan kinerja.

c. **Analisis heuristik** digunakan oleh kedua mesin untuk memastikan bahwa varian dari virus yang tertangkap dengan informasi minim yang tersedia tentang pola kode virus. Analisis heuristik didasarkan pada kenyataan pada program, dokumen atau pesan email yang membawa virus sering memiliki fitur khas. Mereka mungkin mencoba memodifikasi yang tidak diminta oleh file, memanggil mail client, atau menggunakan cara lain untuk mereplikasi diri. Mesin menganalisis kode program untuk mendeteksi jenis-jenis instruksi komputer. Mesin juga mencari kesahan non-virus seperti perilaku sebelum mengambil tindakan anti-virus untuk menghindari menaikkan alarm palsu.

3. Pilihan Ganda Untuk Penanganan Virus.

Administrator memiliki beberapa pilihan untuk menangani pesan yang terinfeksi virus. Seperti virus yang berevolusi, ketegangan serangan baru mencoba untuk memotong perlindungan anti-virus dengan menyembunyikan virus dalam perlindungan password, file dienkripsi atau pesan rusak. Solusi IronPort mendeteksi pesan berpotensi berbahaya, memberikan kontrol penuh administrator atas bagaimana pesan-pesan ini harus ditangani oleh sistem.

4. **Karantina Virus terintegrasi penuh**

Menyediakan opsi tambahan kepada pelanggan untuk menentukan tindakan apa yang dilakukan untuk mengambil pesan-pesan virus bersama dengan pengguna akhir opsi pemberitahuan.

5. **Pintu Gerbang Terukur Dengan Perkembang biakan Terbaik dari Pertahanan Anti-Virus.**

peralatan keamanan IronPort email memungkinkan skalabilitas yang diperlukan untuk sepenuhnya terintegrasi perlindungan anti-virus untuk pertumbuhan pesan lanjutan. Solusi anti-virus juga melindungi Anda dari infrastruktur yang kewalahan oleh wabah virus yang kompleks dan memastikan bahwa misi penting melalui email Anda akan terus diterima.

Manfaat :

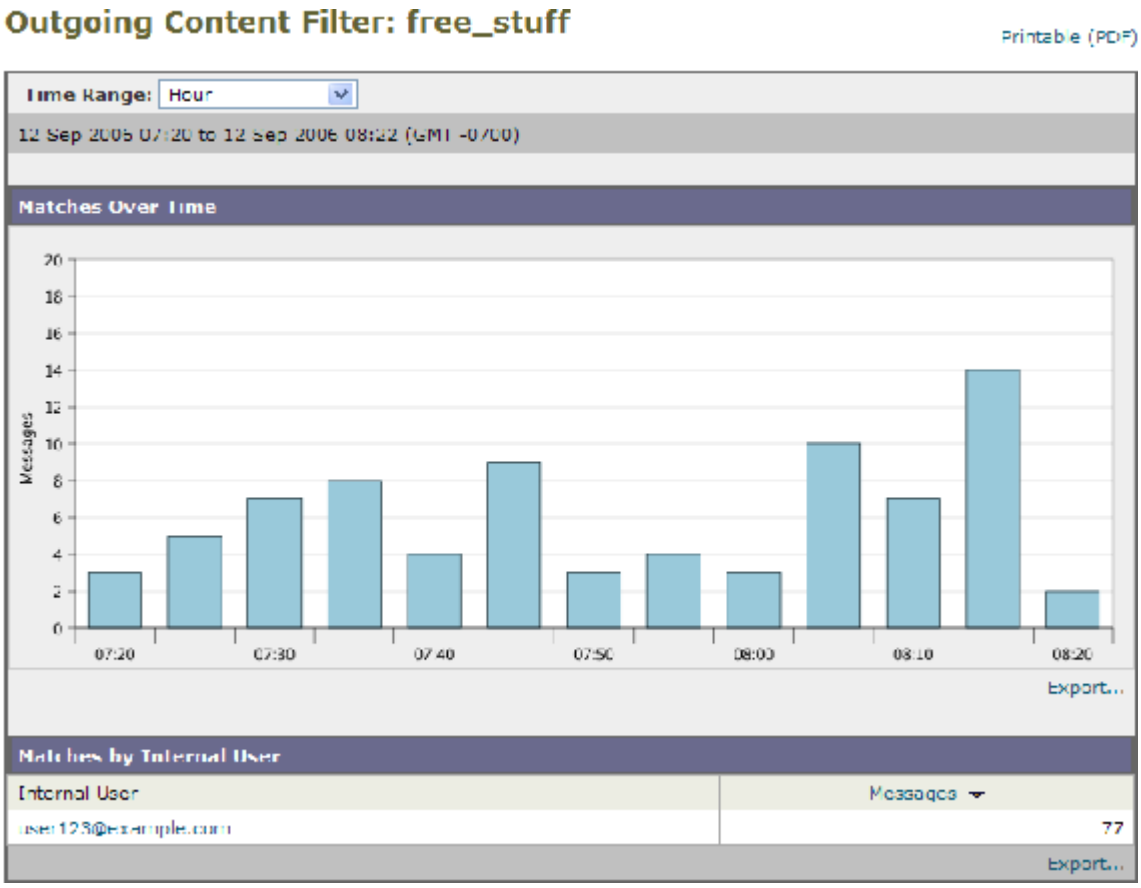
- **Keunggulan tertinggi** dengan menggabungkan Filter Wabah Virus IronPort dengan teknologi anti-virus dari McAfee dan Sophos, peralatan IronPort menyediakan industri terkemuka pencegahan dan perlindungan virus, sambil mempertahankan mendekati angka nol-tingkat positif. Dengan mengintegrasikan beberapa solusi independen, peralatan IronPort memanfaatkan keunggulan masing-masing untuk memberikan keamanan maksimum.

- **Perlindungan Virus yang Terukur** Kinerja tak tertandingi dari peralatan IronPort memastikan skalabilitas yang diperlukan untuk terintegrasi sepenuhnya perlindungan anti-virus untuk melanjutkan pertumbuhan pesan. Kinerja filtering virus pada gateway secara signifikan mengurangi sumber daya yang dibutuhkan pada kelompok perlengkapan server dan kebutuhan bandwidth dalam jaringan.
- **TCO yang lebih rendah dengan Solusi Gateway Terpadu** Dengan manajemen dan penyebaran terpadu dalam peralatan, solusi ini menawarkan kemudahan manajemen dengan update otomatis dan "menetapkan dan melupakan" kebijakan untuk mengatasi kebutuhan setiap pelanggan yang spesifik. Selain itu, virus melakukan filtering pada gateway secara signifikan mengurangi sumber daya yang dibutuhkan pada kelompok peerlenhkapan server dan kebutuhan bandwidth dalam jaringan.

3.2.10 Content Filter

Isi Content Filter menampilkan informasi tentang perbandingan atas konten yang masuk dan keluar filter dalam dua bentuk : *Grafik bar* dan sebuah *daftar*. Mengunakan *Content Filter Page*, anda dapat meninjau kebijakan perusahaan pada basis per-filter konten dan per-user.

Halaman detail *Content Filter* menampilkan filter dari waktu ke waktu, serta oleh pengguna *internal.* Pada bagian pengguna *internal*, anda dapat klik nama pengguna uuntuk melihat halaman rincian pengguna *internal*.



Gambar 3.8 Content Filters Page

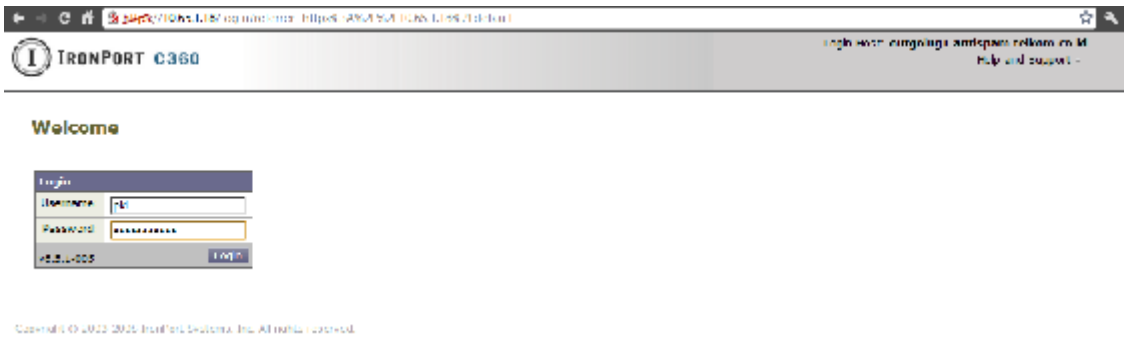
3.3 Tahap Memulai Pengawasan Keamanan Email

Fitur Email security Monitoring terintegrasi erat ke dalam sistem, mengumpulkan data dari setiap langkah dalam proses pengiriman *email* termasuk penyaringan reputasi, pemindaian *anti-spam, anti-virus*, *filter outbrake virus,*

penegakan kebijakan (termasuk filter konten dan pesan pengiriman. Database menindentifikasi dan mencatat setiap pengirim *email* dengan alamat IP, sementara *interfacing* dengan layanan reputasi *SenderBase* untuk real-time informasi identitas. Fitur Email Security monitor memungkinkan tim keamanan untuk menutup lingkaran pada pengirim *email* ke penerima, jumlah *mail* yang dikirim dari dan diterima oleh penerima, dan efektifitas kebijakan keamanan.

Sebelum memulai monitoring email, kita harus login terlebih dahulu :

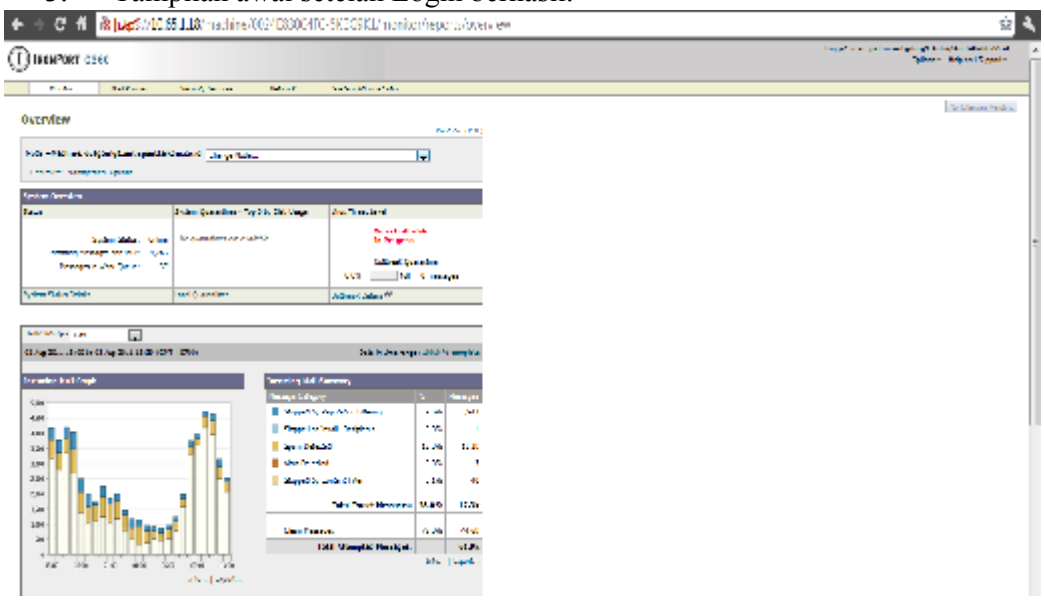
1. Ketik https://10.65.1.18/login?referrer=https%3A%2F%2F10.65.1.18%2Fdefault pada browser anda.
2. Kemudian masukkan User dan Password anda, lalu klik Login.



Gambar 3.9 Login

User dan Password yang kami gunakan khusus bagi mahasiswa yang sedang melakukan aktifitas kerja praktek pada perusahaan PT. Telekomunikasi Indonesia Tbk.

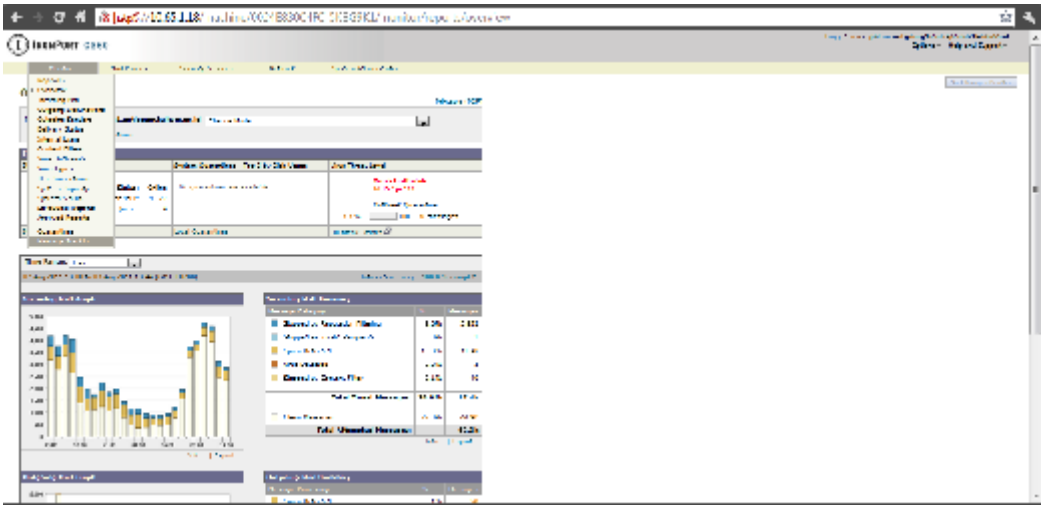
3. Tampilan awal setelah Login berhasil.



Gambar 3.10 Halaman Utama

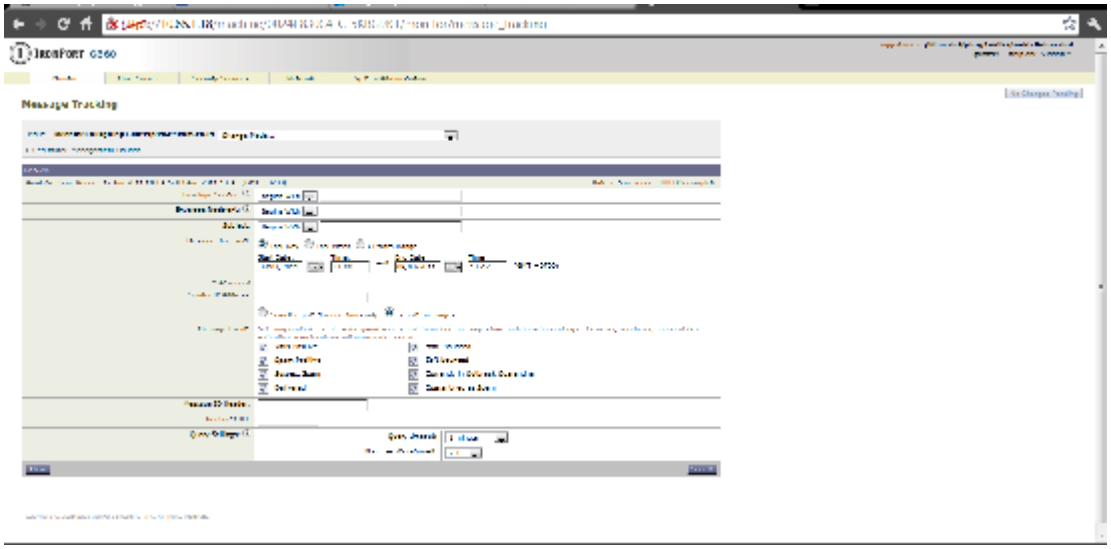
Disini diperlihatkan grafik email yg terdapat gangguan mulai dari email masuk maupun email yg keluar.

4. Pilih menu ‘MONITOR’ kemudian pada sub menu, klik ‘MESSAGE TRACKING’.



Gambar 3.11 Menu Monitor

5. Tampilan Message Tracking.



Gambar 3.12 Message Tracking

Disini merupakan media monitoring mail yang mengalami gangguan dengan ketentuan monitoring yang berfariasi. Monitoring dapat dilakukan sesuai dengan tujuan yang dicapai, monitoring melalui pengirim, penerima dan subjek. Melakukan suatu monitoring dengan secara mempercepat dan membesarkan akurasi pencarian data dapat dilakukan dengan menentukan tanggal pencarian tertentu sesuai yang dibutuhkan.

Bila menginginkan monitoring secara tepat sesuai dengan kesalahan atau gangguan secara objektif dapat dicari dengan media IP address. Dapat juga melakukan monitoring secara pengkatagorian menurut virus positive, spam positive, suspect spam, delivered, hard bounced, soft bounced, currently in outbreak quarantine dan quarantined as spam.

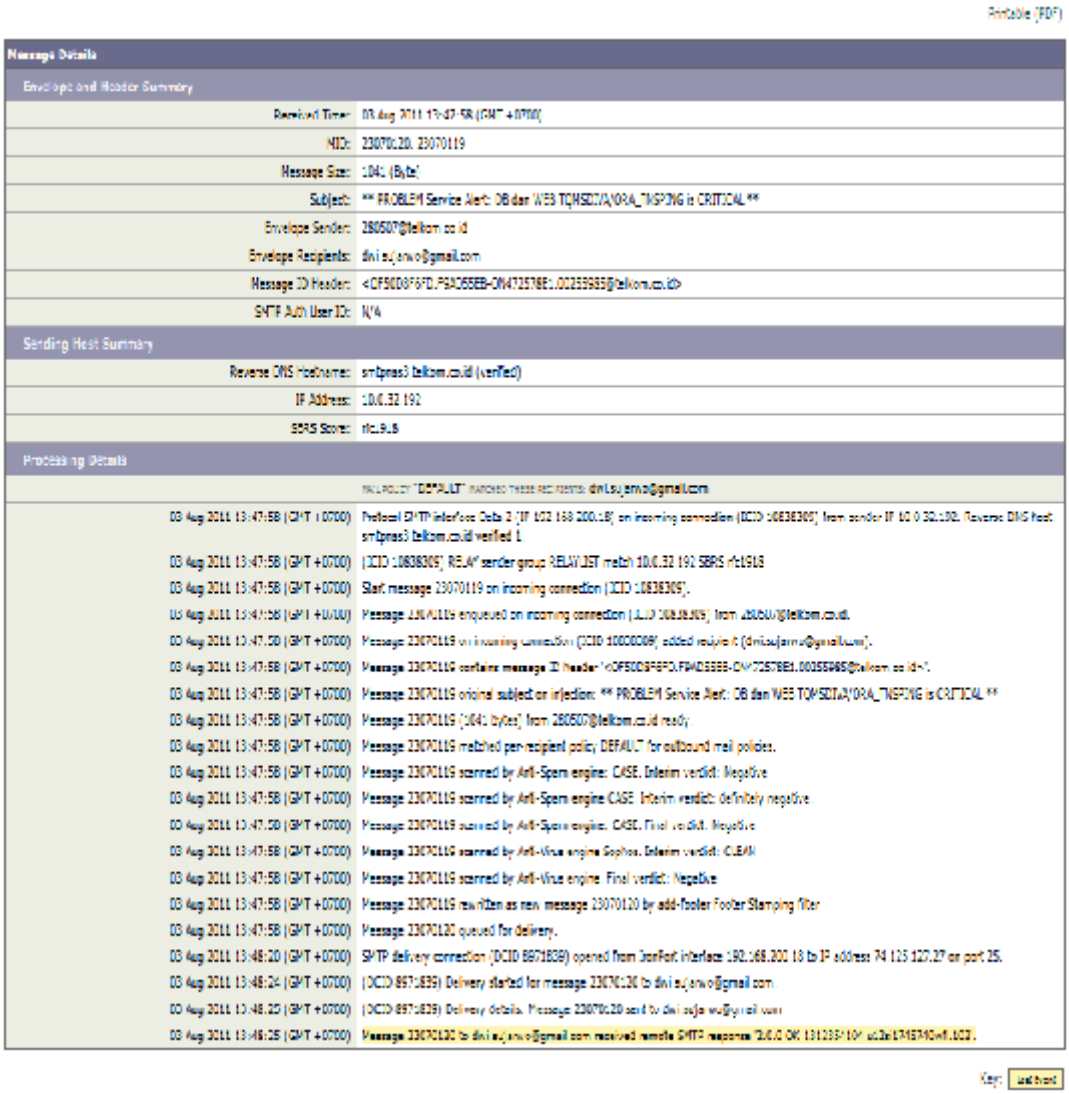
6. Tekan button Search jika ingin memulai scan email.



Gambar 3.13 Pencarian Menurut Katagori

Gambar diatas merupakan hasil pencarian sesuai kebutuhan untuk dapat dilakukannya proses monitoring, maka dapat terlihat status tiap email secara lengkap.

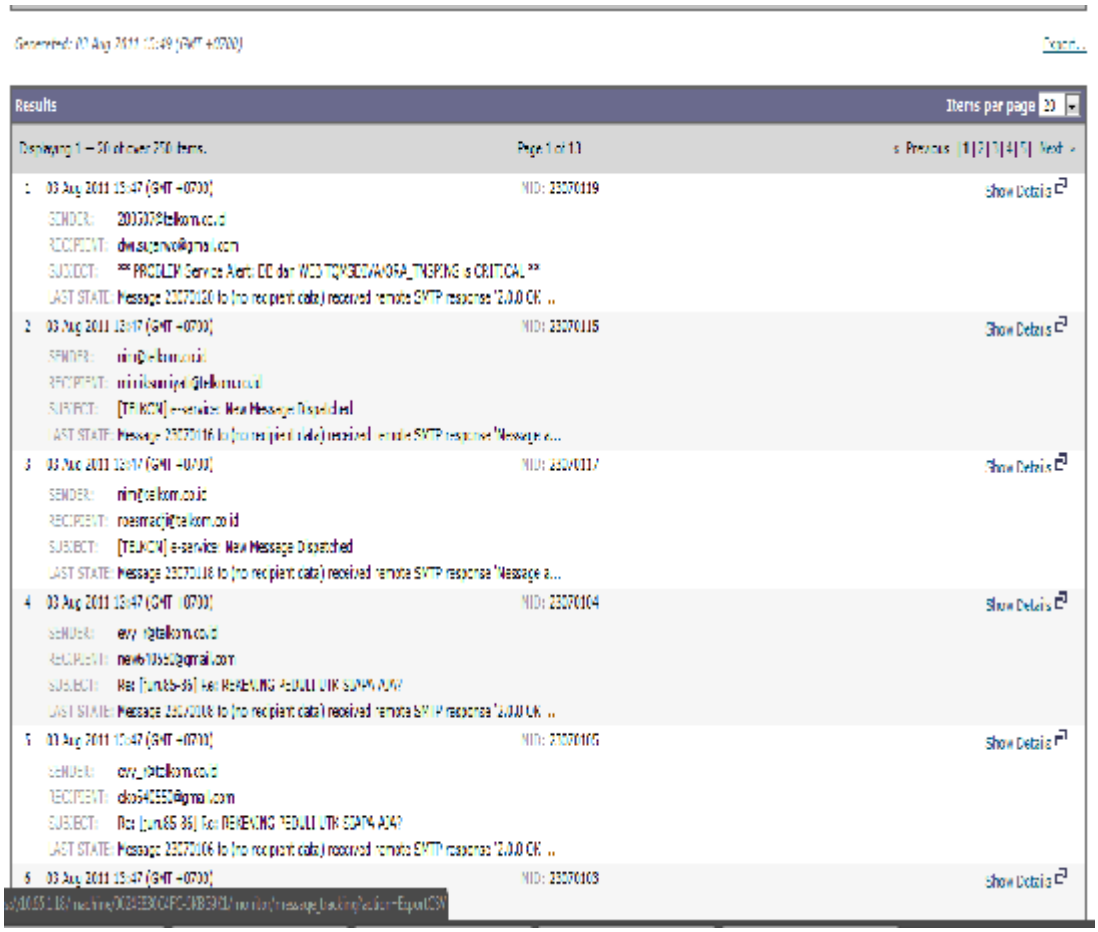
7. Jika ingin melihat detail *email*, tekan ‘Show Detail’.



Gambar 3.14 Detail Email

Untuk dapat melihat status mail secara lengkap dan proses penganalisaan sistem dari awal mail masuk/datang hingga dapat diputuskan masuk kekatagori email yang terdapat gangguan (proses penyaringan/filter).

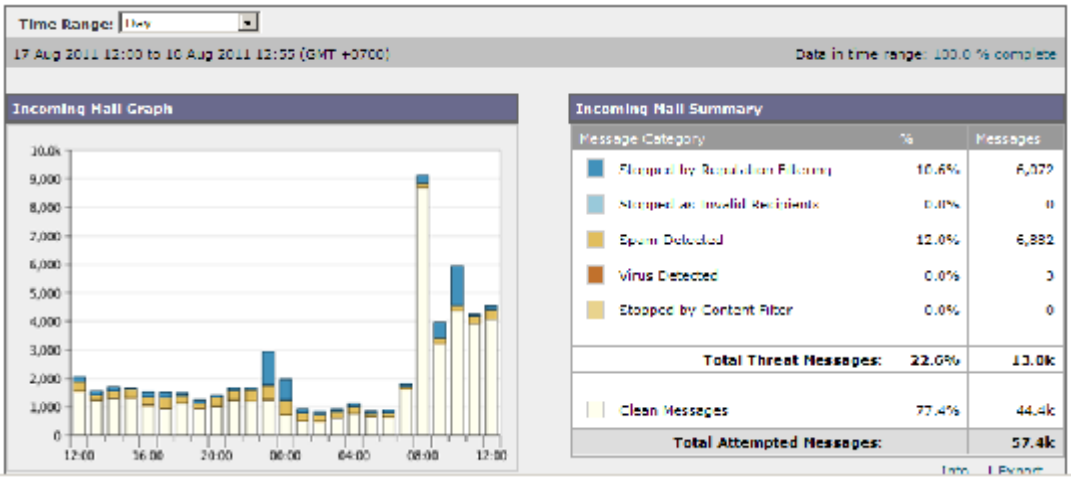
8. Jika ingin mendapatkan hasil print scan, klik ‘Export’.



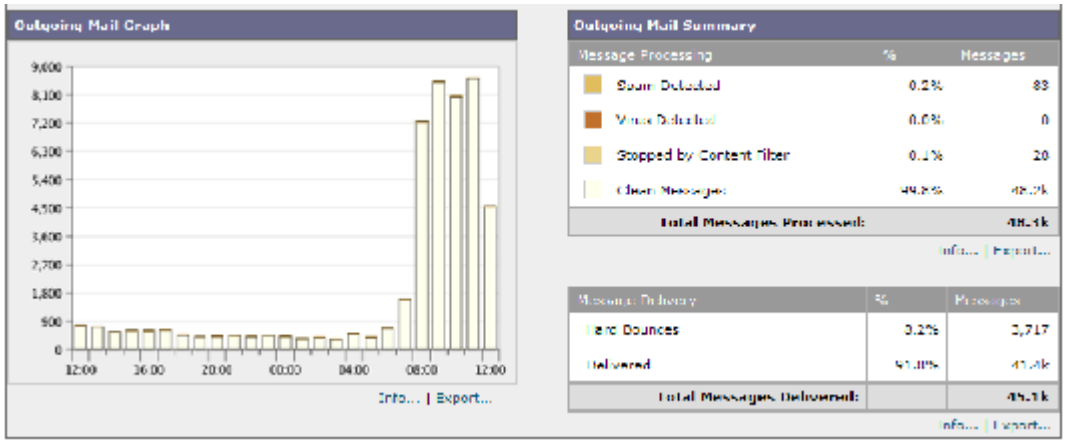
Gambar 3.15 Print Scan

Pada tahap ini sistem memiliki kemampuan penduplikatan data agar dapat dibuatkan laporan untuk dapat diproses lebih lanjut pada pemonitoringan. Penduplikatan dibuatkan dalam format .csv agar mudah dilakukan pengarsipan bagi penggunanya.

Pemonitoringan dilakukan pada bagian overview sebagai penganalisaan email yang masuk mapun keluar (incoming dan outgoing) dengan presentase dan grafik yang dapat ditujukan perharinya :



Gambar 3.16 Incoming Mail



Gambar 3.17 Outgoing Mail

Pada tampilan diatas dapat dilihat pemindaian yang terjadi pada hari tertentu, data akan berubah ditiap waktunya.

3.4 Hasil Monitoring Secara Pengkatagorian

Data pada tabel monitoring ini dilakukan selama sebulan dari bulan Juni - Juli 2011, pada hasil monitoring yang diberikan hanya sebagian dari yang sebenarnya dikarenakan jumlah data yang sangat banyak hingga diambil sebagian.

3.4.1 Delivered

No	Date	MID	Sender	Recipient	Subject	Last State
1	2011-08-03 02:48 GMT	23006836	masgagah80@gmail.com	t_andoko@telkom.co.id,bambangis@telkom.co.id	Revisi: Req ADSL EBIS BR	Message 23006840 to (no recipient data) received remote SMTP response 'Message accepted for delivery'.
2	2011-08-03 02:48 GMT	23006833	(no sender)	admin@gusislam.com	[News Web Infratel] HOT NEWS : Peremajaan Battere STO Godean Arnet Yogyakarta	Message 23006834 to (no recipient data) received remote SMTP response '2.0.0 OK 1312339712 t14si1201192wfg.95'.
3	2011-08-03 02:48 GMT	23006829	harbito.prihantoro@total.com	aribs@telkom.co.id	Draft MoM - TELKOM progress meeting, 29 Juli 2011	Message 23006830 to (no recipient data) received remote SMTP response 'Message accepted for

						delivery'.
4	2011-08-03 02:48 GMT	23006819	sentto-15475040-13205-1312339702-hari_y=telkom.co.id@returns.groups.yahoo.com	hari_y@telkom.co.id	Bls: [InspirasiIndonesia] Kisah Hamdan, Bocah Cilik	Message 23006825 to (no recipient data) received remote SMTP response 'Message accepted for delivery'.
5	2011-08-03 02:48 GMT	23006821	sentto-11651745-221381-1312339701-irwan=telkom.co.id@returns.groups.yahoo.com	irwan@telkom.co.id	Re: [itb76] Birthday Reminder...Uut cs...Tjok besok juga	Message 23006826 to (no recipient data) received remote SMTP response 'Message accepted for delivery'.
6	2011-08-03 02:48 GMT	23006818	(no sender)	admin@gusislam.com	Re: [HaiMedia] Update transaksi DELIMA	Message 23006823 to (no recipient data) received remote SMTP response '2.0.0 OK 1312339711 t14si1201192wfg.95'.
7	2011-08-03 02:48 GMT	23006820	SRS0=mY8TpO=2V=telkom.co.id=710392@srs.bis3.ap.blackberry.com	adilher@telkom.co.id	Apd utk ruang konsul	Message 23006824 to (no recipient data) received remote SMTP response 'Message accepted for

						delivery'.
8	2011-08-03 02:48 GMT	23006811	marketing.paramudya@yahoo.co.id	lazuar@telkom.co.id	=?windows-1252?Q?Operation_&_Manufacturing_Program_August_2011?=	Message 23006814 to (no recipient data) received remote SMTP response 'Message accepted for delivery'.
9	2011-08-03 02:48 GMT	23006810	update+khkmvw-m@facebookmail.com	590021@telkom.co.id	Agus Satriawan juga mengomentari tautan nya.	Message 23006812 to (no recipient data) received remote SMTP response 'Message accepted for delivery'.
10	2011-08-03 02:48 GMT	23006836	masgagah80@gmail.com	t_andoko@telkom.co.id,bambangis@telkom.co.id	Revisi: Req ADSL EBIS BR	Message 23006840 to (no recipient data) received remote SMTP response 'Message accepted for delivery'.

Tabel 3.2 Delivered

Pada pengkatagorian delivered ini merupakan data yang berhasil terkirim kepada penerima atau berhasil melewati pengawasan keamanan. Pada email-email yang termasuk pada delivered ini tidak terjangkit virus maupun spam dan tidak mengalami permasalahan dalam pengiriman maupun penerimaan.

3.4.2 Positive Spam

Date	MID	Sender	Recipient	Subject	Last State
2011-08-03 02:45 GMT	23005987	rtamraiy@stjohnprospect.com	nor@telkom.co.id,edd@telkom.co.id,fushangm@telkom.co.id,har_to@telkom.co.id,deputi_kadivnet@telkom.co.id,mokosh@telkom.co.id	Permanently Enlarge Your Penis At Home.	Message 23005989 quarantined in IronPort Spam Quarantine.
2011-08-03 02:45 GMT	23005970	dude@arcf.com	twahyono@telkom.co.id	Max-Gentleman*Enlargement*Pills	Message 23005972 quarantined in IronPort Spam Quarantine.
2011-08-03 02:44 GMT	23005634	kooovvvvvv10@att.net	nursant@telkom.co.id	Dear Friend.....1	Message 23005637 quarantined in IronPort Spam Quarantine.
2011-08-03 02:43 GMT	23005357	utia@xoxx.com	tursilo@telkom.co.id	Max-Gentleman*Enlargement*Pills	Message 23005358 quarantined in IronPort Spam Quarantine.
2011-08-03 02:43 GMT	23005281	lluo@acbt.com	tua@telkom.co.id	Max-Gentleman*Enlargement*Pills	Message 23005283 quarantined in IronPort Spam Quarantine.
2011-08-03 02:42 GMT	23005235	corp@fis.edu.sg	sutoto@telkom.co.id	=?gb2312?B?cGRudWp2IKH4udwgwO0gtcQgv8Yg0acg0NQg?=\\r\\n\\t=?gb2312?B?0+sg0tUgyvUg0NQgIGxy?=	Message 23005237 quarantined in IronPort Spam Quarantine.
2011-08-03 02:42 GMT	23005225	jiangaj@fzrb.cn	jakal@telkom.co.id	=?utf-8?B?UkU6N2tudiDmiZPpgKDkupTmmJ/nuqfnp5jkuabpq5jnuqfnoJTkv64g?=\\r\\n\\t=?utf-8?B?6JKL5rK75p+P?=	Message 23005226 quarantined in IronPort Spam Quarantine.
2011-08-03 02:42 GMT	23005179	dollylieselotte@philips.com	irwanir@telkom.co.id,herdi@telkom.co.id,waguswin@telkom.co.id,jimur	Fast worldwide shipping and discounted prices. Penis	Message 23005191 quarantined in IronPort

			a@telkom.co.id,pr6o@telkom.co.id, deputy_kadiv_regional_iv@telkom.co.id	Enlargement Pill	Spam Quarantine.
2011-08-03 02:42 GMT	23005063	martinasolange@execulink.com	negaragede@telkom.co.id,memberid_dodiet@telkom.co.id,gxarr@telkom.co.id,ajudi_a@telkom.co.id,s_arto@telkom.co.id,ditjar@telkom.co.id,juwaeni@telkom.co.id,jawati@telkom.co.id,ajpeccievoqtcpqaxhn@telkom.co.id	FDA approved medications. Penis Enlargement Pill - No prescription is required. High Quality is guaranteed!	Message 23005073 quarantined in IronPort Spam Quarantine.

Tabel 3.3 Positive Spam

Positif spam ini dimana email-email dinyatakan sebagai spam. Email yang dinyatakan spam ini akan secara otomatis dikatagorikan oleh perangkat dan akan langsung di karantina hingga data tersebut dapat diatasi. Perangkat akan mengirimkan pesan berupa pemberitahuan kepada administrator bahwa email tersebut dinyatakan spam. Maka langkah selanjutnya diserahkan kepada administrator apakah akan dihapus atau dikirim ulang.

3.4.3 Positive Virus

Date	MID	Sender	Recipient	Subject	Last State
2011-08-03 02:44 GMT	23005638	eka.fajar@cardig.com	sudarmada@telkom.co.id	Pembukaan SLI	Message 23005638 aborted: Dropped by antivirus
2011-08-02 11:11 GMT	22941348	adminsjuip@dhl.com	yustinus@telkom.co.id	DHL Express Delivery cte	Message 22941348 aborted: Dropped by antivirus
2011-08-02	22916372	ulinuha@telkom.co.i	ali.murtado.f@gma	Emailing: zwt.rar	Message 22916372 aborted: Dropped

08:26 GMT		d	il.com		by antivirus
2011-08-01 09:27 GMT	22735326	information@imagichotelreservation.com	uuns@telkom.co.id	Wrong transaction from your credit card in Dunton Hot Springs	Message 22735326 aborted: Dropped by antivirus
2011-08-01 09:25 GMT	22734791	information@lateroo ms.com	kskardha@telkom. co.id	Hotel Plaza Athenee made wrong transaction	Message 22734791 aborted: Dropped by antivirus
2011-08-01 08:46 GMT	22723757	support@booking-hotels.eurobookings. com	sjafwan@telkom.c o.id	Hotel Ritz-Carlton Palm Beach made wrong transaction	Message 22723757 aborted: Dropped by antivirus
2011-07-30 17:18 GMT	22509308	KarenM.NoReply73 @g2gm.com	hid4j4t@telkom.co .id	Proposal Attached	Message 22509308 aborted: Dropped by antivirus
2011-07-29 19:45 GMT	22440787	helping@etaphotel.c om	dart@telkom.co.id	Hotel Ritz-Carlton Orlando, Grande Lakes Resort made wrong transaction	Message 22440787 aborted: Dropped by antivirus
2011-07-29 06:23 GMT	22334409	(no sender)	telkomsurat@gmail .com	Re: Koreksi OLA Task Completion Time DCS	Message 22334409 aborted: Dropped by antivirus
2011-07-29 04:21 GMT	22315311	(no sender)	telkomsurat@gmail .com	Re: Koreksi OLA Task Completion Time DCS	Message 22315311 aborted: Dropped by antivirus

Tabel 3.4 Positive Virus

Pada katagori positif virus ini merupakan email-email yang telah dinyatakan terjangkit virus oleh perangkat. Setiap email yang telah dinyatakan terjangkit virus, maka akan langsung dihapus oleh perangkat dan memberikan informasi kepada administrator bahwa email dihapus dikarenakan email tersebut terjangkit virus.

3.4.4 Quarantine As Spam

Date	MID	Sender	Recipient	Subject	Last State
2011-08-03 02:50 GMT	23007531	haroldtemple@flipag.net	r_ambari@telkom.co.id,tonif@telkom.co.id,muslimah_datel_utara@telkom.co.id	where else are you guaranteed to lose weight, or get your money back.	Message 23007532 quarantined in IronPort Spam Quarantine.
2011-08-03 02:50 GMT	23007492	torydrusilla@tcl.com	dsh@telkom.co.id,putut@telkom.co.id,btridodo@telkom.co.id,b_subagyo@telkom.co.id,mgr_bangsis_dwh_is_center@telkom.co.id,niam@telkom.co.id,fi@telkom.co.id,encang@telkom.co.id,har@telkom.co.id	where else are you guaranteed to lose weight, or get your money back.	Message 23007493 quarantined in IronPort Spam Quarantine.
2011-08-03 02:49 GMT	23007146	benika_kusahika1@yahoo.co.jp	h_maulida@telkom.co.id	From Mrs Benika Kusahiko	Message 23007147 quarantined in IronPort Spam Quarantine.
2011-08-03 02:49 GMT	23007092	elsie@fellowlength.info	amri_pu@telkom.co.id	Refinance Rates Near All-Time Lows - Get Quotes Now	Message 23007093 quarantined in IronPort Spam Quarantine.
2011-08-03 02:48 GMT	23006850	email@profitera.com	didi@telkom.co.id	Collections & Recovery Industry Intelligence	Message 23006855 quarantined in IronPort Spam Quarantine.
2011-08-03 02:48 GMT	23006815	shakirajestine@tcl.com	benyamin@telkom.co.id	0,00E+00	Message 23006817 quarantined in IronPort Spam Quarantine.
2011-08-03 02:48 GMT	23006764	sentto-7302643-177145-1312339693-erdiansyah=telkom.co.id@returns.groups.yahoo.com	erdiansyah@telkom.co.id	[Quadran-I] Jual DVD & VCD Video Sepakbola / Sepak Bola / Football / Soccer	Message 23006771 quarantined in IronPort Spam Quarantine.

2011-08-03 02:48 GMT	23006687	sentto-7302643-177144-1312339683-erdiansyah=telkom.co.id@returns.groups.yahoo.com	erdiansyah@telkom.co.id	[Quadran-I] Young babe Heather Vahn - XXX - 225.53 MB - WUPLOAD and FileSONIC Download	Message 23006688 quarantined in IronPort Spam Quarantine.
2011-08-03 02:48 GMT	23006673	bulahnelle@minmail.net	dwulandari_yk@telkom.co.id	svbab	Message 23006675 quarantined in IronPort Spam Quarantine.
2011-08-03 02:47 GMT	23006603	lezliedinah@health.ne.jp	fietal@telkom.co.id	9d6rra	Message 23006604 quarantined in IronPort Spam Quarantine.

Tabel 3.5 Quarantine As Spam

Quarantine as spam merupakan kumpulan data email yang sudah terduga spam pada perangkat IronPort. Pada katagori ini merupakan email yang belum teratasi oleh administrator dari sebelumnya diatasi pada proses Positif Spam.

3.4.5 Soft Bounced

Date	MID	Sender	Recipient	Subject	Last State
2011-08-03 02:51 GMT	22650551	(no sender)	m.isnaini.saputro@gmail.com	[KALTIMSEL] Fw: [Muslim BPP] "Belajar Tahsin & Hafalan Quran"	Message 22650551 to RID [0] pending until Wed Aug 3 10:51:25 2011 as per bounce profile Default.
2011-08-03 02:49 GMT	22892665	(no sender)	m.isnaini.saputro@gmail.com	Re: ADVERTISE IP LAN >> Fw: Upgrade VPN IP PLN Sektor Mahakam	Message 22892665 to RID [0] pending until Wed Aug 3 10:49:40 2011 as per bounce profile Default.
2011-08-03 02:49 GMT	22892720	(no sender)	m.isnaini.saputro@gmail.com	PERFORMANCE REPORT GEOSERVICES Juli 2011	Message 22892720 to RID [0] pending until Wed Aug 3 10:49:37 2011 as per bounce profile Default.

2011-08-03 02:49 GMT	22892824	(no sender)	m.isnaini.saputro@gmail.com	DELIVERY FAILURE: Error delivering to noc08/mitra/multimedia/Telkom; Router: Database\\r\\n disk quota exceeded	Message 22892824 to RID [0] pending until Wed Aug 3 10:49:35 2011 as per bounce profile Default.
2011-08-03 02:49 GMT	22728775	(no sender)	m.isnaini.saputro@gmail.com	DELIVERY FAILURE: Error delivering to ServiceDesk Jkt09/400213/Telkom; Router: Database\\r\\n disk quota exceeded	Message 22728775 to RID [0] pending until Wed Aug 3 10:49:34 2011 as per bounce profile Default.
2011-08-03 02:49 GMT	22892822	(no sender)	m.isnaini.saputro@gmail.com	DELIVERY FAILURE: Error delivering to NOC20/mitra/multimedia/Telkom; Router: Database\\r\\n disk quota exceeded	Message 22892822 to RID [0] pending until Wed Aug 3 10:49:18 2011 as per bounce profile Default.
2011-08-03 02:49 GMT	22892285	(no sender)	m.isnaini.saputro@gmail.com	RE: [REQ CP & SISKA] SUPRA UNI LAND UTAMA/TRIJAYA PRATAMA FUTURES VPN IP 512KBPS (SUPPORT)	Message 22892285 to RID [0] pending until Wed Aug 3 10:49:08 2011 as per bounce profile Default.
2011-08-03 02:49 GMT	22889742	(no sender)	m.isnaini.saputro@gmail.com	RE: SIMULASI TARGET RABU>>>MODIFY P2P KE MP2MP AKSES METRO @25MB U/ IP TRANSIT SATNETCOM PLUS ORDER BACK UP AKSES METRO LINK KST	Message 22889742 to RID [0] pending until Wed Aug 3 10:49:02 2011 as per bounce profile Default.
2011-08-03 02:48 GMT	22946804	c4agent242@telkom.co.id	c4d1@milis.telkom.co.id	FW: Problem Bandarjaya Proklamator TT:M.0802.10871	Message 22946804 to RID [4] pending until Wed Aug 3 10:48:17 2011 as per bounce profile Default.

2011-08-03 02:47 GMT	22727182	(no sender)	m.isnaini.saputro@gmail.com	DELIVERY FAILURE: Error delivering to ServiceDesk Jkt18/400222/Telkom; Router: Database\\r\\n disk quota exceeded	Message 22727182 to RID [0] pending until Wed Aug 3 10:47:48 2011 as per bounce profile Default.

Tabel 3.6 Soft Bounced

Pada katagori soft bounced ini, email yang dikirim mengandung illegal host/domain name tidak ditemukan, pengirim mencoba untuk mengirim pesan dengan tidak ada alamat penerima atau alamat penerima tidak valid. Maka perangkat akan mengirim kembali email tersebut kepada pengirim dengan kurun waktu yang telah ditentukan.

Pada saat kerja praktek terjadi bouncing kepada email salah satu pegawai, dimana email yang dikirim dikembalikan lagi kepada pengirim. Setelah dianalisis pada perangkat (terdapat informasi terjadinya bounced) diketahui bahwa waktu dan tanggal pengiriman email tidak sesuai dengan waktu dan tanggal pada perangkat.

3.4.6 Suspect Spam

Date	MID	Sender	Recipient	Subject	Last State
2011-08-03 02:48 GMT	23006764	sentto-7302643-177145-1312339693-erdiansyah=telkom.co.id@returns.groups.yahoo.com	erdiansyah@telkom.co.id	[Quadran-I] Jual DVD & VCD Video Sepakbola / Sepak Bola / Football / Soccer	Message 23006771 quarantined in IronPort Spam Quarantine.

2011-08-03 02:42 GMT	23005229	lakehome@host.cybermatrixllc.biz	iswanti@telkom.co.id	Breaking News: Clickbank Millionare Confesses to Being Homeless!	Message 23005230 quarantined in IronPort Spam Quarantine.
2011-08-03 02:24 GMT	23000445	a_yuliani@telkom.co.id	aniek.telkomsmg@gmail.com	Fw: Obat Leukemia Gratis	Message 23000448 quarantined in IronPort Spam Quarantine.
2011-08-03 02:22 GMT	22999838	email@profitera.com	aguskris@telkom.co.id	Collections & Recovery Industry Intelligence	Message 22999840 quarantined in IronPort Spam Quarantine.
2011-08-03 02:19 GMT	22999213	email@profitera.com	alex_js@telkom.co.id	Collections & Recovery Industry Intelligence	Message 22999215 quarantined in IronPort Spam Quarantine.
2011-08-03 02:13 GMT	22998043	litoretita@yahoo.com	humala@telkom.co.id	(no subject)	Message 22998044 quarantined in IronPort Spam Quarantine.
2011-08-03 02:13 GMT	22997754	sentto-14202064-131538-1312337581-erdiansyah=telkom.co.id@returns.groups.yahoo.com	erdiansyah@telkom.co.id	[toserba] Get welknown & legal American degree from "UNIVERSITY OF BERKLEY, MICHIGAN, USA " either by attending clss or by distance learning from any part of the world. via LMII who has a License from Department Pendidikan on each city where LMII has office.	Message 22997756 quarantined in IronPort Spam Quarantine.
2011-08-03 02:12 GMT	22997610	sentto-7302643-177142-1312337549-erdiansyah=telkom.co.id@returns.groups.yahoo.com	erdiansyah@telkom.co.id	[Quadran-I] Kareena Kapoor, topless with chocolate over her boobs - 18 pics	Message 22997614 quarantined in IronPort Spam Quarantine.
2011-08-03 02:06 GMT	22996141	terrapinn@sg.terrapinnmedia.com	junkom@telkom.co.id	ZXP Series 3 - Low cost-per-card high speed direct-to-card	Message 22996144 quarantined in IronPort Spam Quarantine.

				printer! (ADV)	
2011-08-03 01:51 GMT	22993134	magnoliashira@honeywell.com	nager_kancatel_kendal@telkom.co.id	36o	Message 22993137 quarantined in IronPort Spam Quarantine.

Tabel 3.7 Suspect Spam

Dalam katagori ini merupakan pemberitahuan email yang diduga terjangkit spam. Setelah email diduga spam oleh perangkat maka email tersebut akan dikarantina dan perangkat akan memberikan pesan kepada pengirim yang menyatakan bahwa email tersebut terjangkit spam.