PERTANYAAN YANG SERING DIAJUKAN
TENTANG PEREKAMAN TRANSAKSI KONEKSI

Bagaimana perkembangan pelaksanaan perekaman transaksi koneksi?

Sesuai tugas dan fungsi pokok ID-SIRTII di dalam Permen Menkominfo 26/2007 di bidang log file adalah bersifat pasif. Demikian juga dalam SOP yang diatur melalui Kepdirjen 227/2007, ID-SIRTII berfungsi hanya menerima rekaman transaksi koneksi dari ISP dan kemudian mengelola penyimpanannya untuk dipergunakan dalam rangka proses penegakan hukum apabila dibutuhkan. Untuk itu ID-SIRTII menyiapkan server dan aplikasi penerimaan rekaman transaksi koneksi.

Untuk mendorong ISP dalam melaksanakan kewajibannya, maka ID-SIRTII telah memfasilitasi uji coba implementasi perekaman transaksi koneksi di sejumlah ISP (Telkom, Indosat M2, CBN, Centrin, NapInfo, Biznet, Indonet dan XL).

Apa konsekuensi dan implikasi teknis pelaksanaan kewajiban ini bagi ISP?

Implementasi pengumpulan Log File menimbulkan konsekuensi teknis yang kompleks bagi ISP sehingga memerlukan waktu dan uji coba maupun untuk realisasinya:

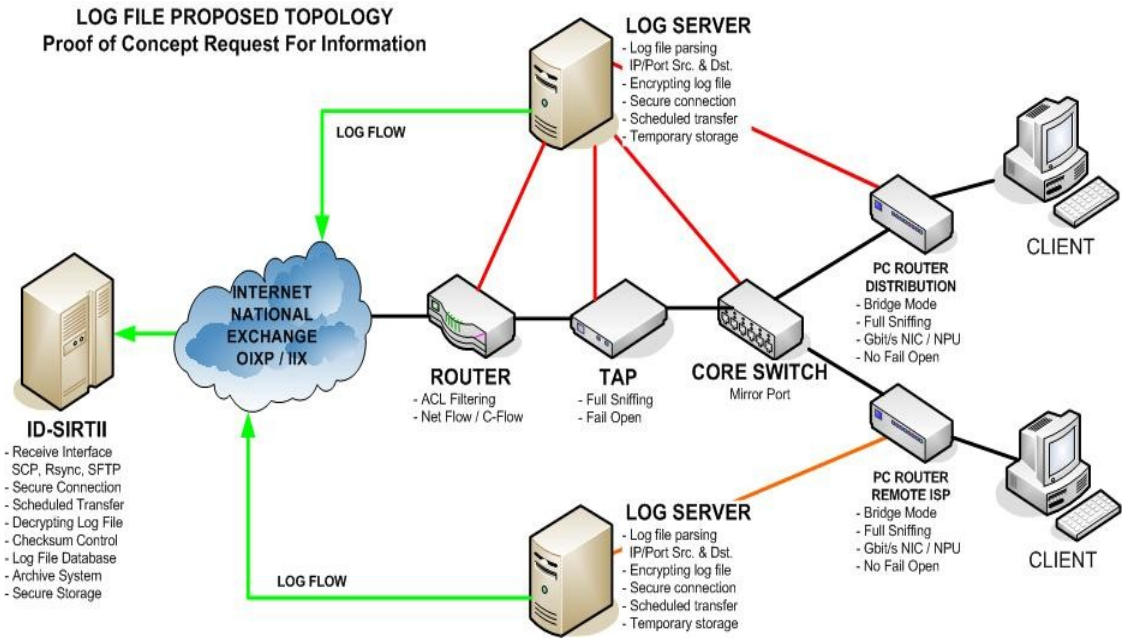
1. Terlebih dahulu perlu dilakukan standarisasi format log, penamaan log, kode dan sinkronisasi waktu server dan perangkat jaringan ISP sesuai time server;
2. Rekonfigurasi perangkat router yang membutuhkan kecermatan, trial dan error, yang mungkin dapat mengganggu keberlangsungan dan kualitas layanan;
3. Penambahan fungsi untuk menangkap traffic log kemungkinan besar akan dapat berakibat menurunkan (degradasi) performa perangkat secara signifikan sehingga dapat berakibat pada keberlangsungan layanan;
4. Walaupun hanya untuk uji coba, mungkin perlu pengadaan perangkat baru atau update kapasitas perangkat. Apabila benar-benar diimplementasi akan lebih banyak lagi perangkat yang perlu diupgrade, biayanya akan signifikan;
5. Perlu pengadaan server log dan development aplikasi parsing log, sehingga sesuai dengan kebutuhan: ip/port source, ip/port destination dan time stamp.

Apakah ada permasalahan non teknis dari ISP?

1. Masih sering terjadi kesalahpahaman dan kerancuan pengertian antara pemantauan traffic dan perekaman transaksi koneksi. Kemungkinan ini terjadi karena manajemen ISP belum atau tidak memahami sepenuhnya aspek teknis pelaksanaan kewajiban ini dan kekhawatiran berlebihan terhadap kemungkinan penyalahgunaan data perusahaan dan pelanggan dan isu penyadapan;
2. Seringnya pergantian personil kontak resmi yang dikirimkan oleh NAP dan ISP untuk mengikuti pembahasan mengakibatkan pemahaman yang tidak lengkap dan tidak tersampaikannya informasi dan data yang tepat mengenai pelaksanaan kewajiban, aspek teknis dan regulasinya;
3. Komitmen yang telah disepakati perlu birokrasi panjang di dalam internal perusahaan untuk dilaksanakan. Sementara tidak semua yang terkait ikut terlibat secara langsung dan terus menerus di dalam pembahasan. Sehingga, dalam kasus tertentu, manajemen telah menyetujui dan teknis bahkan sudah melaksanakan, tapi pihak legal masih mempertanyakan. Seharusnya ini tidak perlu terjadi bila di

dalam perusahaan ada koordinasi yang baik.

Seperti apa konsep teknis implementasi perekaman transaksi koneksi?



Konsep Implementasi Teknis Perekaman Transaksi Koneksi

Ada sejumlah konsep usulan model implementasi pengumpulan log file:

1. Menangkap traffic log langsung pada router utama (gateway) dan dikirimkan ke log server yang terpisah. Kelemahannya: hanya traffic log antara network internal dan external yang tertangkap, sedangkan traffic log antar network client tidak tertangkap dan kemungkinan besar performa perangkat router utama akan turun yang dapat mengganggu keberlangsungan layanan dan kemungkinan terjadinya down time. Alternatif metode yang digunakan adalah memanfaatkan fungsi Access List Filtering (ACL) atau menggunakan fungsi protokol Net Flow (Cisco), C-Flow (Juniper) – untuk mengolah protokol ini diperlukan tambahan aplikasi lain;
2. Menangkap traffic log pada router distribusi terdekat dengan network client dan dikirimkan ke log server yang terpisah dan diletakkan di NOC. Kelemahannya: ada banyak router yang harus menjalankan fungsi ini dan untuk pengiriman log ke log server akan mengorbankan bandwith backhaul antara router distribusi ke NOC serta kemungkinan besar performa perangkat router distribusi akan turun yang dapat mengganggu keberlangsungan layanan. Alternatif metode yang digunakan adalah memanfaatkan fungsi Access List Filtering (ACL) atau menggunakan fungsi protokol Net Flow (Cisco), C-Flow (Juniper) – untuk mengolah protokol ini diperlukan tambahan aplikasi lain;
3. Model paling ideal adalah memasang perangkat TAP/Mirror sebelum router distribusi sehingga tidak mengganggu performa jaringan ISP dan perangkat router agar layanan tetap terjaga. Kelemahannya: perlu investasi dalam jumlah banyak untuk mengadakan perangkat TAP/Mirror dan untuk pengiriman log file ke log server akan mengorbankan bandwith backhaul antara router distribusi ke NOC;
4. Perangkat TAP/Mirror bisa digantikan dengan PC Router dengan mode bridge,

sehingga dapat ditingkatkan kapasitas dan kemampuan komputasinya dengan mudah dan murah dibandingkan dengan membeli perangkat TAP/Mirror maupun meningkatkan spesifikasi router. Kelemahannya PC Router tidak memiliki fitur Fail Open sehingga apabila terjadi hardware failure, link layanan akan mengalami gangguan (interupsi) dan terjadi down time. Akan tetapi solusi PC Router bisa menjadi pilihan yang sesuai untuk ISP kecil di daerah;

5. Hasil pengamatan, asumsi volume logs yang akan disimpan (tanpa kompresi):
   - Untuk setiap 1 Mbit/s traffic normal akan menghasilkan rata-rata 4 KBytes logs
   - Rata-rata traffic Internet Indonesia saat peak adalah 8 Gbit/s = 32 MBytes
   - Volume logs yang akan dihasilkan 320 GBytes / hari = 9 TBytes / bulan.

   Perlu alokasi kapasitas penyimpanan dan bandwidth untuk mengirim logs.

Berapa perkiraan biaya dan investasi yang diperlukan oleh ISP?

Harga perangkat TAP/Mirror cukup mahal, tergantung kapasitasnya. Berkisar antara 7 – 20 juta rupiah per unit. Sedangkan berdasarkan uji coba yang pernah dilakukan oleh ID-SIRTII, spesifikasi log server minimal kelas prosesor Dual Xeon, RAM 4 GB dilengkapi dengan Harddisk SCSI dengan kapasitas > 200 GB. Harganya berkisar 30 – 40 juta rupiah per unit.

Untuk PC Router spesifikasinya bisa lebih rendah tergantung volume traffic serta jumlah paket yang ditangani (Packet Per Second – PPS), misalnya Dual/Quad Core Processor, RAM 4 GB dengan Network Interface Card (NIC) kecepatan tinggi (Gbit/s) atau yang memiliki fitur NPU (Network Processing Unit) untuk meningkatkan skalabilitas. Harga PC Router berkisar antara 3 – 6 juta rupiah per unit.

Bagaimanakah pendapat dan tanggapan ISP terutama di daerah?

Hasil pemetaan dan diskusi dengan ISP daerah dari beberapa kali kunjungan untuk sosialisasi menghasilkan kesimpulan: ISP daerah memiliki terbatasnya sumber daya, dari segi kemampuan perangkat, skill teknis serta finansial. Terutama bila digunakan model implementasi no. 3 (ISP daerah sebagai titik distribusi yang terdekat dengan network client yang akan paling bertanggung jawab terhadap implementasi og file).

Apa kesepakatan teknis antara ID-SIRTII dengan ISP?

Dengan 8 ISP besar telah dicapai kesepakatan antara lain:

1. Terlebih dahulu akan melakukan penyelarasan waktu perangkat jaringan yang ada dan belum ditentukan kapan akan dilakukan dan sampai kapan batasnya karena menunggu dikeluarkannya ketetapan dari Dirjen Postel. Akan tetapi ISP sepakat untuk secara bertahap melakukan inisiatif penuelarasan waktu tanpa menunggu keluarnya Peraturan Dirjen Postel;
2. Disepakati format untuk pewaktuan adalah **HH:MM:SS** (durasi 24 jam) dan penanggalan **DD/MM/YYYY**;
3. Masing-masing ISP masih memerlukan pemetaan dan diskusi pembahasan lebih lanjut di sisi internal untuk menentukan pilihan model implementasi perekaman transaksi koneksi yang paling tepat untuk kondisi masing-masing;
4. Sejumlah ISP besar telah melakukan uji coba implementasi metode perekaman transaksi koneksi ini dengan meminjam perangkat TAP milik ID-SIRTII;

5. Diupayakan untuk berbagi informasi data teknis seperti besaran log file serta performa sistem berdasarkan inisiatif ISP besar yang melakukan uji coba;
6. Diadakan rapat rutin pembahasan log file dan Tim Koordinasi Respon Insiden 2 x setiap bulan yaitu hari Jumat minggu pertama dan hari Jumat minggu ketiga.

Apa alternatif rekomendasi pelaksanaan kewajiban ini?

Pada dasarnya, kewajiban ini harus tetap dilaksanakan mengingat pentingnya peran log file dalam proses penegakan hukum. Akan tetapi harus tetap dipertimbangkan efektifitas implementasinya, agar jangan sampai justru membebani atau bahkan menghambat pertumbuhan industri Internet. Untuk itu ada beberapa pendekatan untuk mengurangi beban tersebut dengan asumsi ISP bersedia melakukan investasi:

1. Salah satu faktor yang membebani implementasi kewajiban ini, terutama untuk ISP daerah adalah ketersediaan kapasitas bandwith untuk pengiriman. Sehingga, akan lebih efektif dan efisien apabila log tersebut disimpan sementara di lokal ISP. Untuk itu perlu payung regulasi yang memungkinkan ISP memiliki kewenangan tersebut dan tata cara (standar dan prosedur) yang memungkinkan penyimpanan yang sah dan dapat dipertanggungjawabkan di dalam proses penyidikan sehingga oleh hakim di pengadilan dapat diterima sebagai alat bukti yang sah;
2. Perlu jadwal pentahapan yang ketat untuk memastikan semua ISP dapat segera melaksanakan kewajiban ini dan diberikan asistensi teknis untuk implementasinya dan dimulai dari ISP skala besar (bisnis dan jaringan) sebagai percontohan;
3. Setiap pengajuan ISP baru dan ISP yang sedang tahap Uji Laik Operasi sudah dipersyaratkan untuk memasukkan desain teknis dan skema investasi untuk implementasi kewajiban perekaman transaksi koneksi;
4. Untuk memperkuat dan melengkapi kewajiban perekaman transaksi koneksi ini, perlu diterbitkan regulasi yang mengatur kewajiban bagi penyelenggara layanan konten untuk juga melaksanakan kewajiban serupa;
5. Diterbitkan panduan teknis model implementasi perekaman transaksi koneksi berdasarkan best practices yang pernah dilakukan.