

PANDANGAN HUKUM DAN TEKNIS TENTANG ID-SIRTII



**DIRJEN POS DAN TELEKOMUNIKASI
DEPARTEMEN KOMUNIKASI DAN
INFORMATIKA**

DAFTAR ISI



1. **Aspek Legal ID-SIRTII**
2. **Aspek Teknis ID-SIRTII**

DAFTAR ISI



- 1. Aspek Legal ID-SIRTII**
2. Aspek Teknis ID-SIRTII

ASPEK LEGAL ID-SIRTII



**UU 36 TAHUN 1999 TENTANG
TELEKOMUNIKASI**

BERKAITAN DENGAN PEMBINAAN



UU No.36 tahun 1999 tentang Telekomunikasi Pasal 4

- Bahwa Telekomunikasi dikuasai oleh Negara dan pembinaannya dilakukan oleh Pemerintah. Pembinaan telekomunikasi diarahkan untuk meningkatkan penyelenggaraan telekomunikasi yang meliputi penetapan kebijakan, pengaturan, pengawasan dan pengendalian. Dalam penetapan kebijakan, pengaturan, pengawasan dan pengendalian di bidang telekomunikasi, dilakukan secara menyeluruh dan terpadu dengan memperhatikan pemikiran dan **pandangan yang berkembang dalam masyarakat serta perkembangan global.**
- Bahwa telekomunikasi di kuasai oleh Negara dan pembinaannya di lakukan oleh Pemerintah Mengingat telekomunikasi merupakan salah satu cabang produksi yang penting dan strategis dalam kehidupan nasional, maka penguasaannya dilakukan oleh negara, yang dalam penyelenggaraannya ditujukan untuk sebesar-besarnya bagi kepentingan dan kemakmuran rakyat.

Berkenaan dengan Penyelenggaraan Telekomunikasi yang dijadikan dasar ID-SIRTII



UU no.36 tahun 1999 tentang Telekomunikasi Pasal 7

- Dalam penyelenggaraan telekomunikasi, diperhatikan hal-hal sebagai berikut:
 - a. melindungi kepentingan dan keamanan negara;**
 - b. mengantisipasi perkembangan teknologi dan tuntutan global;**
 - c. dilakukan secara profesional dan dapat dipertanggungjawabkan;**
 - d. peran serta masyarakat.**

ASPEK LEGAL ID-SIRTII



**PERATURAN MENTERI KOMUNIKASI DAN
INFORMATIKA
NO.26/PER/M.KOMINFO/5/2007 TENTANG
PENGAMANAN PEMANFAATAN JARINGAN
TELEKOMUNIKASI BERBASIS PROTOKOL
INTERNET**

Berkenaan dengan Aktivitas Monitoring dan Pengumpulan Log



Peraturan Menteri Komunikasi dan Informatika No.26/PER/M.KOMINFO/5/2007

- Rekaman aktifitas transaksi koneksi (log file) adalah suatu file yang mencatat akses pengguna pada saluran akses operator/ penyelenggara jasa akses berdasarkan alamat asal protocol internet (source), alamat tujuan (destination), Jenis protocol yang di gunakan, port asal (source), Port tujuan (destination) dan waktu (time stamp) serta durasi terjadinya Transaksi
- Monitoring jaringan adalah fasilitas pemantau dan pendeteksi pola (pattern) dan transaksi yang berpotensi mengganggu atau menyerang jaringan untuk tujuan memantau kondisi jaringan, memberikan peringatan dini (early warning) dan melakukan tindakan pencegahan (prevent)

TUGAS ID-SIRTII



1. Mensosialisasikan kepada seluruh pihak yang terkait untuk melakukan kegiatan pengamanan, pemanfaatan jaringan telekomunikasi berbasis protocol internet
2. Melakukan pemantauan, pendeteksian dini dan peringatan dini terhadap ancaman dan gangguan pada jaringan telekomunikasi berbasis protocol internet (monitoring)
3. Membangun dan atau menyediakan, mengoperasikan, memelihara dan mengembangkan sistem database pemantauan dan pengamanan pemanfaatan jaringan telekomunikasi berbasis protocol internet sekurang-kurangnya untuk:
 - ✦ Mendukung kegiatan sebagai mana dimaksud dalam butir b; (pemantauan, pendeteksian dini dan peringatan dini terhadap ancaman dan gangguan pada jaringan telekomunikasi berbasis protocol internet di Indonesia).
 - ✦ Menyimpan rekaman transaksi (log file).Mendukung proses penegakan hukum

TUGAS ID-SIRTII



1. Melaksanakan Fungsi layanan informasi atas ancaman dan gangguan keamanan pemanfaatan jaringan telekomunikasi berbasis protocol internet
2. Menyediakan laboratorium simulasi dan pelatihan kegiatan pengamanan pemanfaatan jaringan telekomunikasi berbasis protocol internet
3. Melakukan konsultasi dan layanan public
4. Menjadi contact point dengan lembaga terkait tentang pengamanan pemanfaatan jaringan telekomunikasi berbasis protocol internet baik dalam negeri maupun luar negeri

DAFTAR ISI



1. Aspek Legal ID-SIRTII
- 2. Aspek Teknis ID-SIRTII**

ASPEK TEKNIS ID-SIRTII



PARTISIPASI PENGAMANAN INTERNET

Partisipasi Pengamanan Internet ?



- Network Time Protocol (NTP- *time server*)
- Perekaman transaksi koneksi (log)
 - Format log yang diperlukan
 - Tata cara penyampaian log
- Network Monitoring (di level NAP)
- Registrasi pengguna Hotspot, Internet Prabayar, Warung Internet dan akses menggunakan telepon selular

ASPEK TEKNIS ID-SIRTII



STANDARISASI WAKTU

NTP



- ID-SIRTII akan menyediakan 2 buah time server yang akan disinkronisasikan ke **id.pool.ntp.org**
- Masing-masing ISP wajib melakukan sinkronisasi waktu server ke server NTP **id.pool.ntp.org**
- Masing-masing ISP wajib membuka NTP Server untuk diakses komputer dalam jaringannya

Kesepakatan Format Waktu



- DD/MM/YYYY
- HH:MM:SS (24 jam)
- 3 wilayah waktu, WIB, WITA, WIT
- Alamat NTP **id.pool.ntp.org**
- 2 server diregister dalam pool
- Akan ditetapkan oleh Peraturan Dirjen

ASPEK TEKNIS ID-SIRTII



KEWAJIBAN PENGIRIMAN LOG FILE

Bentuk Log (Permen 26/2007)



- Bentuk log yang harus dicatat berupa :
 - IP Address asal
 - IP Address tujuan
 - Nomor Port asal
 - Nomor Port tujuan
 - Informasi protokol yang digunakan
 - Waktu (tanggal dan jam)

Penyadapan?

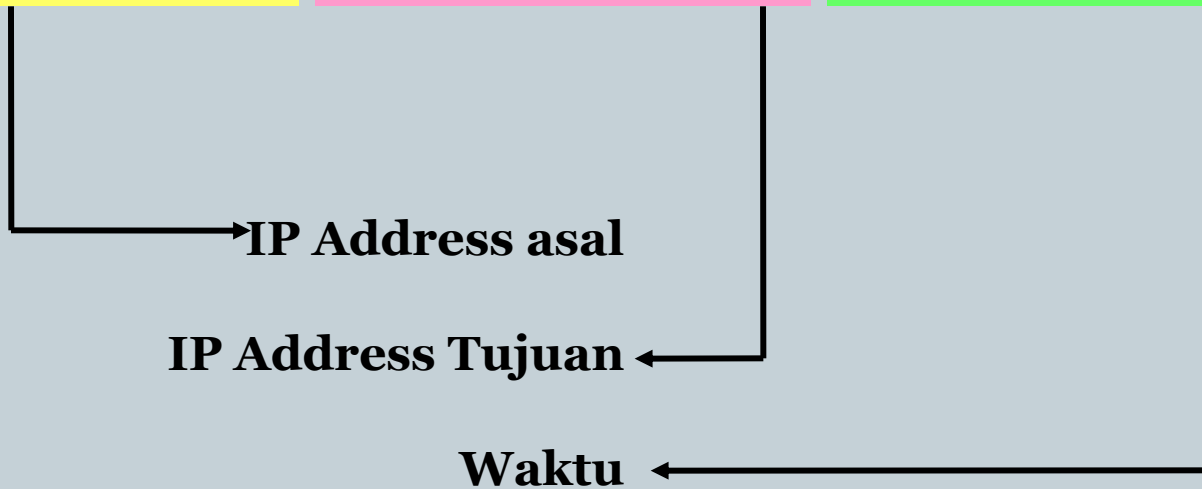


- Proses pencatatan log bukan penyadapan
 - Hanya mencatat IP, port, protokol dan waktu
 - Bisa dilakukan akumulasi log untuk satu IP asal dan IP tujuan yang sama, sepanjang diketahui waktu mulai dan berakhirnya akses (aplikasi filter)
 - Content **bukanlah** hal yang dimonitor
 - Analogi: Operator telepon mencatat nomor asal dan nomor telepon tujuan, tapi tidak merekam percakapan atau isi SMS yang dikirimkan / diterima

Contoh Log



202.155.0.1	202.153.246.1	01/12/2008 10:09:05
203.175.0.1	202.155.246.1	01/12/2008 10:09:07
204.157.0.1	202.165.246.1	01/12/2008 10:09:09
205.159.0.1	202.115.246.1	01/12/2008 10:09:11



Beda Sistem Log & Monitoring



- Log dicatat di mesin log ISP dan ditangkap di mesin router/switch distribusi yang terdekat dengan end users network untuk menangkap bukti insiden yang terjadi antar client & insiden pada level exchange
- Berbeda dengan sistem monitoring yang ada di level gateway network internasional (NAP) dan national exchange (OpenIXP dan IIX)

Detail Pengiriman Log



- Cara pengiriman log secara otomatis dari server log ISP ke server penerima ID-SIRTII dengan menggunakan metode SCP, SFTP dan standar pengiriman secure data lainnya
- Jika dibutuhkan software tambahan seperti sniffer untuk dipasang pada server / pc router, maka ID-SIRTII akan membantu untuk pengembangan software tersebut

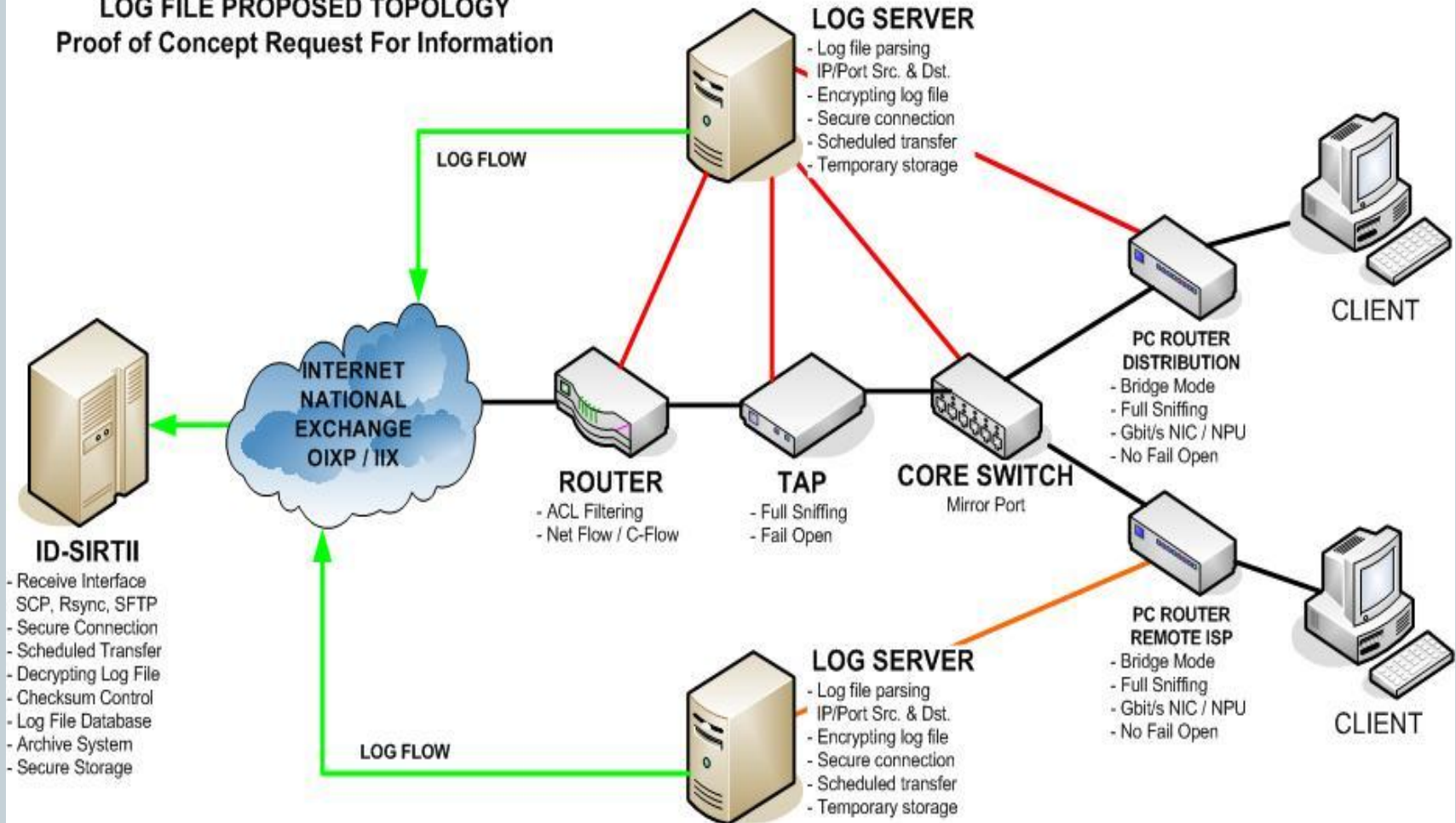
Sistem Pengiriman Log



- Secara Otomatis, online streaming dengan penjadwalan ke server penerima ID-SIRTII sesuai jumlah ISP dan volume log
- Secara Berkala, offline dalam format digital dikirimkan melalui pos tercatat / kurir
- Tata cara pengiriman log diatur di dalam Peraturan Dirjen Postel 227/2007

Desain Implementasi

LOG FILE PROPOSED TOPOLOGY Proof of Concept Request For Information



Implikasi Teknis



- Standarisasi format & sinkronisasi waktu
- Rekonfigurasi & uji coba – down time
- Terjadi degradasi performa perangkat
- Perlu upgrade & atau pengadaan baru
- Perlu server log & development aplikasi
- Perlu mengalokasikan bandwidth khusus
- Perlu mengalokasikan storage khusus

Regulasi Berikutnya



- Modern licensing: syarat ISP baru & ULO
- Kewajiban serupa pada content provider

ASPEK TEKNIS ID-SIRTII



MONITORING

Network Monitoring



- Monitoring Network dilakukan pada titik-titik kritis di Internet Exchange dan NAP
- Monitoring dilakukan dengan pemasangan perangkat sensor (IDP) secara pasif
- Penyelenggara Internet Exchange dan NAP wajib membuka akses dan menyediakan fasilitas penempatan perangkat sensor
- Diatur dalam Perdirjen 225/2008

ASPEK TEKNIS ID-SIRTII



PENCATATAN IDENTITAS

Pencatatan Identitas



- Penyelenggaraan hotspot / wireless access point / bentuk open public access network lainnya seperti warnet dan kampus, harus dilakukan dengan adanya mode otentikasi, sehingga dapat dilakukan registrasi identitas pengguna
- Sedang disusun draft Perdirjen tentang kewajiban pencatatan identitas pengguna akses publik

Format Pencatatan Identitas



- Nomor kartu identitas (SIM, KTP dll.)
- Nama lengkap (opsional: nama kecil, julukan)
- Alamat lengkap (opsional: nomer telepon, hp)
- Jenis kelamin, Tanggal lahir, Pekerjaan, Status
- Catatan waktu akses (mulai, berakhir, durasi)
- Catatan terminal akses dan IP yang dipakai
- Opsional: copy kartu identitas dan atau foto