BAB II

TINJAUAN PUSTAKA

2.1. Profil Tempat Kerja Praktek

2.1.1 Sejarah Instansi

PT Industri Telekomunikasi Indonesia (Persero) yang berdiri pada tanggal 30 Desember 1974 melalui Keputusan Menteri Keuangan No. 1 Kep. 1971/MK/1974 tertanggal 28 Desember 1974. Serta Akta Notaris Latief No. 232 adalah Badan Usaha Milik Negara (BUMN) yang bergerak di bidang industri khususnya sektor telekomunikasi dan elektronika profesional.

Pada awal pengelolaannya PT Industri Telekomunikasi Indonesia (Persero) disingkat PT INTI (Persero) berada di bawah Depertemen Perhubungan. Kemudian sejak tahun 1983 berada di bawah Departemen Pariwisata dan Telekomunikasi (Deparpostel) dan melalui Keppres No. 44 tahun 1989, PT INTI (Persero) dimasukan dalam kelompok Industri Strategis yang berada dalam lingkungan BPIS (Badan Pengelola Industri Strategis). Sejak berdirinya sampai sekarang PT INTI (Persero) berkedudukan di Jalan Moh. Toha No 77 dan Jalan Moh. Toha No. 255 Bandung. Dalam perkembangannya PT INTI (Persero) memiliki cabang yang terletak di Gedung BNI lantai 18 Jalan Jendral Sudirman Ka. 1 Jakarta dan Jalan Prapanca No. 15 Surabaya.

Sejarah perkembangan PT INTI (Persero) dibagi dalam beberapa periode :

1. Periode sebelum tahun 1945

Pada tahun 1982 didirikan laboratorium Pos, Telepon, dan Telegraf (PTT) di daerah Tegalega (sekarang Jalan Moh. Toha No. 77 Bandung). Pada tahun 1929 didirikan laboratorium radio dan pusat perlengkapan radio, yang kemudian laboratorium ini merupakan bagian terpenting untuk penelitian dan pengembangan tetekomunikasi Indonesia.

2. Periode tahun 1945 -1960

   Setelah perang dunia II selesai, laboratorium pos, telepon, dan telegraf serta laboratorium radio ditingkatkan kedudukannya menjadi laboratorium telekomunikasi yang mencakup segala bidang, yaitu bidang pos, telepon, telegraf, dan radio. Sedangkan bengkel pusat perlengkapan radio diubah menjadi bengkel pusat telekomunikasi.

3. Periode tahum 1960 -1969

   Pada periode ini ditandatangani kerjasama antara Perusahaan Negara Telekomunikasi dengan SIEMENS AG pada tanggal 25 Mei 1966. Pelaksanaannya diberikan kepada Lembaga Penelitian dan Pengembangan Pos dan Telekomunikasi (LPP POSTEL), yang kemudiam dirubah namanya menjadi Lembaga Penelitian dan Pengembangan Industri Pos dan Telekomunikasi (LPPI POSTEL). Untuk merealisasikan kerjasama tersebut, maka pada tanggal 12 Januari 1968 dibangun pabrik telepon, dan pada tanggal 22 Juni 1968 pabrik tersebut diresmikan pembukaannya oleh Menteri EKUIN Sri Sultan Hamengku Buwono IX.

4. Periode tahun 1969 – 1979

Periode ini diadakan rapat kerja pos dan telekomunikasi di Jakarta pada tanggal 1 sampai dengan 3 Oktober 1970. Hasil dari rapat tersebut adalah LPPI POSTEL dalam waktu 4 tahun harus mempersiapkan diri untuk dapat berdiri sendiri di bidang keuangan, kepegawaian, dan peralatan. Sejalan dengan perkembanganya perusahan, maka pada tahun 1971 diadakan pemisahan dalam LPPI POSTEL, yaitu:

1. Lembaga Penelitian dan Pengembangan Pos dan Telekomunikasi mempunyai tugas pokok dalam bidang pengujian, penelitian, dan pengembangan sarana pos dan telekomunikasi baik dari segi teknologinya maupun dari segi operasionalnya.
2. Lembaga Industri (Produksi) sebagai badan hukum yang berdiri sendiri mempunyai tugas pokok memproduksi sarana-sarana atau alat-alat telekomunikasi sesuai dengan kebutuhan nasional.

Pada tanggal 8 Maret 1973 Menteri Perhubungan mengeluarkan Surat Keputusan No. 32 KM 32/R/Phd-73 yang menetapkan langkah-langkah antara lain :

1. Dalam tubuh Lembaga Penelitian dan Pengembangan Industri Pos dan Telekomunikasi oleh Presiden RI tanggal 22 Juni 1968.
2. Untuk keperluan di atas ditentukan bentuk usaha dan bentuk hukum yang sebaik-baiknya hingga mendapatkan fasilitas yang cukup dalam lingkungan Lembaga Penelitian dan Pengembangan Pos dan Telekomunikasi.
3. Pada tahun 1972 Struktur Organisasi LPPI POSTEL dirubah menjadi Lembaga Penelitian dan Pengembangan Pos dan Telekomunikasi (LPP POSTEL).

4. Sehubungan dengan hal ini dianggap perlu apabila bagian industri telekomunikasi ditetapkan sebagai Proyek Industri Telekomunikasi dengan pimpinan proyek Ketua Lembaga Penelitian dan Pengembangan Pos dan Telekomunikasi.

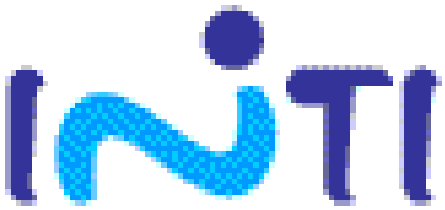
Adapun maksud dan tujuan didirikannya Proyek Telekomunikasi, yaitu :

1. Meningkatkan hasil-hasil produksi dalam negeri yang berupa alat-alat telekomunikasi, baik untuk memenuhi kebutuhan Perusahaan Umum Telekomunikasi (Perumtel) maupun badan organisasi lainnya yang ada di Indonesia atau keperluan ekspor.
2. Peningkatan devisa bagi kebutuhan alat-alat atau perangkat telekomunikasi.
3. Membuka lapangan kerja baru yang dapat menampung sejumlah tenaga kerja.

Pada tahun 1974 dikeluarkan Peraturan Pemerintah RI No. 34 tentang penyertaan modal negara untuk pendirian telekomunikasi yang ada pada Departemen Perhubungan pada saat itu, dijadikan suatu badan pelaksana kegiatan produksi alat-alat telekomunikasi. Untuk kelancaran pelaksanaan pendiriannya sesuai dengan ketentuan pasal 2 ayat 1 Peraturan Pemerintah No.12 Tahun 1969, maka penyertaan modal negara dalam rangka pendirian perusahaan perseroan diatur dengan peraturan negara. Berdasarkan Keputusan Menteri Keuangan RI No. 1 Kep 1771/Mk/Vi/1974 tanggal 28 Desember 1974 serta Akta Notaris Abdul Latief, Jakarta No. 232, maka Proyek Telekomunikasi Indonesia (Persero) disingkat PT INTI (Persero) terhitung sejak tanggal 30 Desember 1974, dengan modal dasar perseroan sebesar Rp 3.200.000.000,00

dan modal perusahaan sebesar Rp 1.600.000.000,00 serta modal yang disetorkan sebesar Rp 900.000.000,00.

2.1.2 Logo Instansi



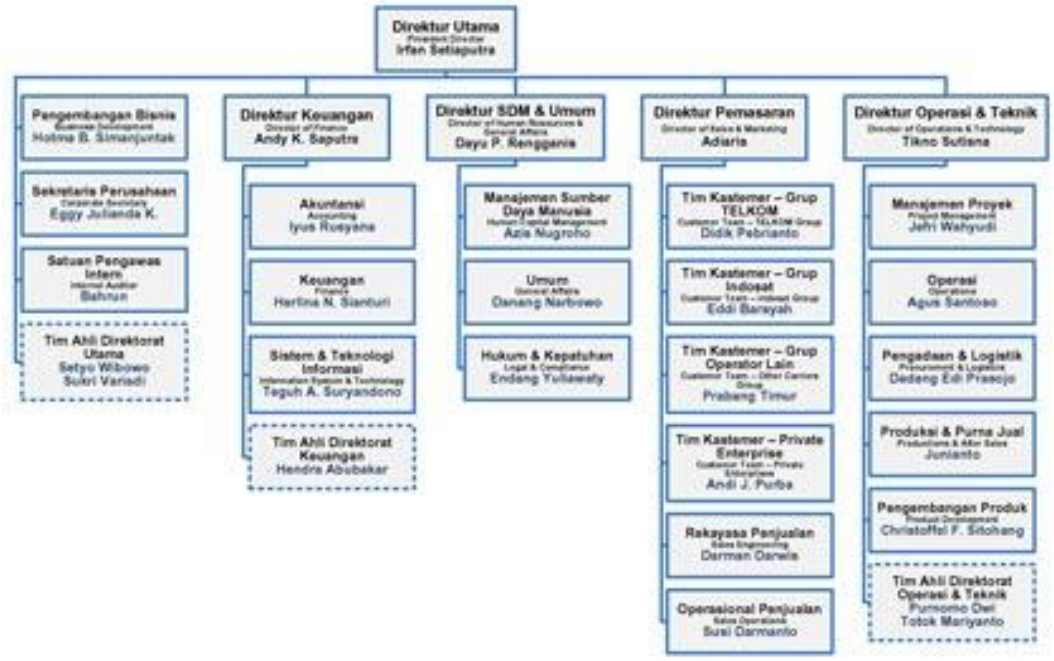
Gambar 2.1 Logo PT.INTI

2.1.3 Badan Hukum Instansi

PT Industri Telekomunikasi Indonesia (Persero) yang berdiri pada tanggal 30 Desember 1974 melalui Keputusan Menteri Keuangan No. 1 Kep. 1971/MK/1974 tertanggal 28 Desember 1974. Serta Akta Notaris Latief No. 232 adalah Badan Usaha Milik Negara (BUMN) yang bergerak di bidang industri khususnya sektor telekomunikasi dan elektronika profesional.

2.1.4 Struktur Organisasi dan Job Description

2.1.4.1 Struktur Organisasi



Gambar 2.2 Struktur Organisasi Perusahaan

2.1.4.2 Job Description

Divisi di PT. INTI (persero) terbagi menjadi 5 divisi dimana divisi-divisi dibentuk dengan tujuan untuk mendukung kelancaran kegiatan korporasi dan *Stategic Business Unit* dalam rangka mencapai tujuan perusahaan yang telah ditetapkan, divisi tersebut diantaranya :

1) Divisi Sekretariat

   Merencanakan, melaksanakan, dan mengendalikan kegiatan-kegiatan untuk memberikan dukungan umum dalam kaitannya dengan bidang hukum, kehumasan, sistem informasi, perencanaan perusahaan, penyelenggaraan ketatausahaan perkantoran umum sesuai dengan ketentuan-ketentuan perusahaan.

2) Divisi SDM dan Umum

Merencanakan, melaksanakan, dan mengendalikan serta mengembangkan pengelolaan sumber daya manusia dan organisasi berdasarkan strategi perusahaan serta melaksanakan kegiatan pengamanan lingkungan perusahaan dan pengolahan fasilitas kerumahtanggaan kantor pusat.

3) Divisi Keuangan

Merencanakan, melaksanakan, dan mengendalikan pengelolaan keuangan serta sistem akuntansi perusahaan berdasarkan kebijaksanaan strategi perusahaan.

4) Divisi *Quality Assurance*

Merencanakan, melaksanakan dan mengendalikan kehandalan mutu fungsi barang dan jasa yang dihasilkan perusahaan, untuk meningkatkan produktivitas perusahaan berdasarkan kebijaksanaan strategi perusahaan.

5) Divisi Penelitian dan Pengembangan

Melakukan penerobosan-penerobosan baru maupun inovasi untuk menciptakan produk-produk baru, pengembangan atas produk-produk yang sudah ada serta melakukan kerjasama dengan mitra asing maupun lokal dalam rangka *transfer technology* dan *technical know how*.

2.1.4.3 Bidang Pekerjaan Perusahaan

Ruang lingkup bisnis INTI difokuskan pada penyediaan jasa dalam bidang informasi dan telekomunikasi atau infokom, yang terdiri dari:

Infrastructure Development Support

Infocom Operations & Maintenance Support

Infocom System & Technology Integration

Infocom Total Solution Provider

Selain itu, INTI juga melakukan penjualan produk software dan produk dan jasa multimedia.

Sesuai dengan perkembangan teknologi dan tuntutan pasar, INTI membagi kegiatan bisnisnya menjadi empat bidang kegiatan sebagai berikut:

Jaringan Telekomunikasi Tetap (JTT)

Jaringan Telekomunikasi Selular (JTS)

Jasa Integrasi Teknologi (JTT)

Jaringan Telekomunikasi Privat (JTP)

Outside Plant (OSP)

Product, Market, and Competence of INTI

Product	**Market**	**Competence**
Fixed Telecommunication Network (JTT)	*Fixed Telecommunication Operator*	System Integration Fixed Network Narrowband and Wideband

Cellular Telecommunication Network (JTS)	*Cellular Telecommunication Operator*	*System Integration* *Cellular Network* *Narrowband and Wideband*
Technology Integration Service (JIT)	*Telecommunication Operator, Corporate & Public*	*Original Products and Capability* *Engineering Design* *Network Management Tools* *CPE (Customer Premises Equipment)* *CME (Civil, Mechanical and Electrical)* *Technology Solution*
OutSide Plant (OSP)	*Fixed & Cellular Telecommunication Operator*	*Installation & Maintenance* *Cabling/Wiring* *Ducts, poles, towers, repeaters etc.* *Fixed & Cellular Network*

Tabel 2.1 ***Product, Market, and Competence***

2.2 Landasan Teori

2.2.1 Sistem Informasi

2.2.1.1 Keamanan Sistem Informasi

Keamanan sistem informasi adalah cabang studi dari teknologi informasi yang mengkhususkan diri untuk mempelajari metode dan gteknik untuk melindungiinformasi dan sistem informasi dari akses, penggunaan, penyebaran, perusakan, perubahan, dan penghancuran tanpa otorisasi yang sah. Bidang ilmu ini berupaya untuk memperhatikan 3 buah aspek yang sangat pentingdalam hal keamanan informasi. 3 aspek tersebut adalah :

1. Kerahasiaan(*confidentiality*). Aspek ini berkaitan dengan pembatasan akses ke sebuah informasi kecuali pihak yang memiliki otorisasi untuk mengaksesnya.

2. Integritas(*integrity*). Aspek ini berkaitan dengan keakuratan dan kelengkapan sebuah informasi dan metode pemrosesannya.

3. Ketersediaan(*availability*). Aspek ini berkaitan dengan ketersediaan informaasi jika suatu pihak dengan otorisasi yang benar berusaha mengaksesnya.

Aspek – aspek tersebut harus selalu dalam keadaan seimbang dalam penerapan usaha pengamanan informasi sebuah organisasi. Jika terdapat ketimpangan disalah satu aspek keamanan data,

maka praktik pengamanan yang dilakukan akan menghambat jalannya bisnis organisasi seperti biasa.

Implementasi usaha pengamanan informasi harus memiliki sebuah panduan dan kontrol agar memiliki tujuan dan dasar pengambilan keputusan yang jelas. Panduan-panduan yang dapat dibuat untuk mengarahkan usaha pengamanan informasi ke arah yang sesuai dengan tujuan organisasi dapat dituangkan dalam bentuk kebijakan, prosedur, praktek operasional, struktur organisasi, serta fungsi perangkat lunak. Rincian dari panduan ini ditentukan melalui sebuah aktifitas analisa resiko untuk mengidentifikasi tingkat keperluan dan kerawanan sebuah aset informasi.

2.2.1.2 Strategi Keamanan Sistem Informasi

Strategi keamanan sistem informasi adalah sebuah rencana yang disusun untuk menanggulangi resiko dan sesuai dengan aturan legal, pemerintah, kontrak, dan kebutuhan internal. Langkah-langkah yang dapat dilakuan dalam penyusunan strategi adalah :

1. Pendefinisian sasaran kontrol keamanan
2. Identifikasi dan penaksiran untuk seluruh pendekatan solusi yang memenuhi sasaran kontrol keamanan

3. Pemilihan metode kontrol keamanan
4. Penetapan nilai patokan dan ukuran
5. Persiapan implementasi kontrol dan rencana pengujian

Strategi keamanan informasi mencakup tindakan pencegahan, pendeteksian, dan respon. Ketiga aspek tersebut harus ada untuk sebuah kerangka keamanan informasi yang handal dan kopmrehensif. Umumnya sebuah strategi keamanan memfokuskan sumber dayanya kepada usaha pencegahan dibandingkan pendeteksian dan respon.

Strategi kaamanan informasi harus menetapkan sebuah pembatasan hak akses dan pembatasan aktifitas yang tidak memiliki otorisasi. Konsep isi dudukung dengan penerapan domain keamanan, least permissions, dan least privilege.

Pembuatan domain keamanan melibatkan perancangan sebuah jaringan yang dapat mengelompokkan pengguna dan sumber daya secara logika ataupun fisik. Selain itu seperangkat kontrol yang efektif harus diterapkan untuk menanggulangi resiko yang relavan terhadap tiap-tiap domain. Teknologi yang dapat digunakan untuk memaksakan aturan ini antara lain firewall, virtual LAN, Access Control List, dan direktori. Konsep least permissin dan least privilege digunakan untuk memfasilitasi fungsionalitas namun tetap membatasi aksi-aksi yang dapat membahayakan sistem.

2.2.2 Router

Router adalah sebuah peralatan komputer yang didedikasikan untuk meneruskan sebuah paket data antara jaringan komputer. Fungsi utama router adalah untuk memutuskan jalur routing mana yang harus diambil agar paket yang diterima oleh router tersebut dapat sampai ke alamat tujuannya.

Router seperti perangkat keras komputer lain, harus memiliki sebuah sistem operasi agar bisa menjalankan fungsi yang sudah ditentukan sebelumnya. Namun tidak seperti sistem operasi untuk perangkat komputer biasa, router memiliki sistem operasi khusus (*proprietary*) yang cukup kecil, aman dan terkostumasi untuk tugas routing. Sistem operasi dari router ini yang kemudian menjadi wadah bagi seluruh kegiatan penyaluran paket data beserta penerapan ACL.

2.2.3 Sistem Operasi Router

Router berdiri diatas sebuah sistem operasi yang berperan untuk melakukan manajemen memory dan input/output. Penggunaan versi sistem operasi router yang tepat harus dilakukan dengan mempertimbangkan kebutuhan dari jaringan organisasi dan tingkat kematangan versi sistem operasi tersebut.

2.2.4 Virtual Private Network (VPN)

Virtual private network adalah sebuah jaringan maya / virtual yang berdiri diatas jaringan komputer lainnya, yang memiliki mekanisme

pengamanan lebih ketat untuk komunikasi datanya jika dibandingkan jaringan komputer biasa. Mekanisme yang terlibat dalam pengamanan data di dalam sebuah VPN adalah autentikasi, kontrol akses, pengecekan integritas data, serta enkripsi. Tingkat keamanan yang ditawarkan oleh VPN memungkinkan pengguna untuk mengirimkan data yang sensitif melalui sebuah jaringan yang tidak dipercaya seperti internet.

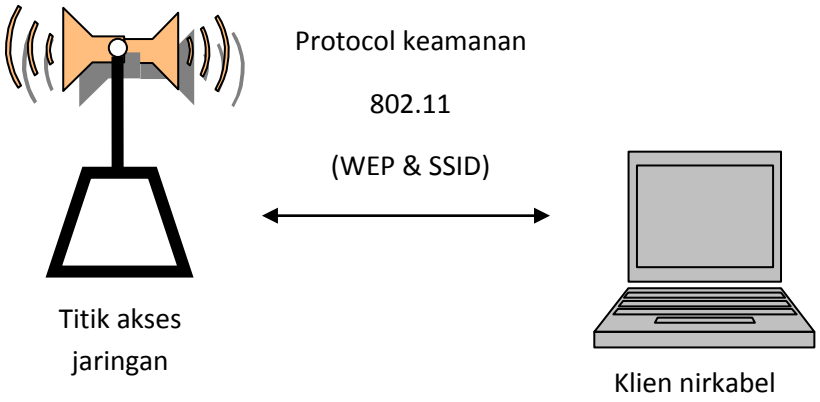
Implementasi VPN saat ini dapat menggunakan IPSec, SSL/TLS, atau L2TP sebagai metode keamanan dan enkripsi paket data. Metode-metode pengamanan ini dapat menggunakan beberapa alternatif teknik enkripsi dalam melakukan komunikasi secara aman dari satu titik ke titik lain. Teknik kriptografi yang digunakan untuk melakukan enkripsi data lain DES, 3DES atau AES. Kemudian untuk melakukan autentikasi dan pengecekan integritas data dapat menggunakan algiritma hashing seperti HMAC MD5 dan SHA-1.

Meskipun VPN memiliki metode pengamanan yang lengkap, terdapat beberapa kelemahan yang dapat menihilkan seluruh usaha keamanan yang dilakukan.

2.2.5 Jaringan nirkabel

Jaringan nirkabel adalah jaringan lokal yang terbangun tanpa koneksi kabel secara fisik. Perangkat komputer dapat berkomunikasi antara satu dengan yang lain dengan menggunakan gelombang radio. Beberapa standar dan spesifikasi yang digunakan unguk membangun jarigan nirkabel ini

adalah IEEE 802.1a/b/g/n, OpenAir, HiperLAN, Bluetooth dan HomeRF. Diantara standar-standar ini, IEEE 802.1g adalah yang paling luas diimplementasikan oleh organisasi.



Gambar 2.3 Topologi Jaringan Nirkabel

Penggunaan jaringan nirkabel saat ini mulai banyak dilakukan oleh organisasi bisnis, pemerintah dan pengguna rumahan. Keuntungan yang ditawarkan oleh teknologi ini adalah penghilangan penggunaan kabel fisik yang terkadang memerlukan biaya dan usaha implementasi yang tidak sedikit.

Service Set Identifier (SSID) yang digunakan untuk mengontrol akses kedalam jaringan nirkabel umumnya desebarkan secara broadcast dan dalam teks yang jelas. Teknik wierd equivalency privacy (WEP) yang digunakan untuk melakukan enkripsi komunikasi memiliki kelemahan dalam desain dan algoritmanya sehingga dapat dipcahkan dalam waktu yang relatif cepat.

2.2.6 Proxy

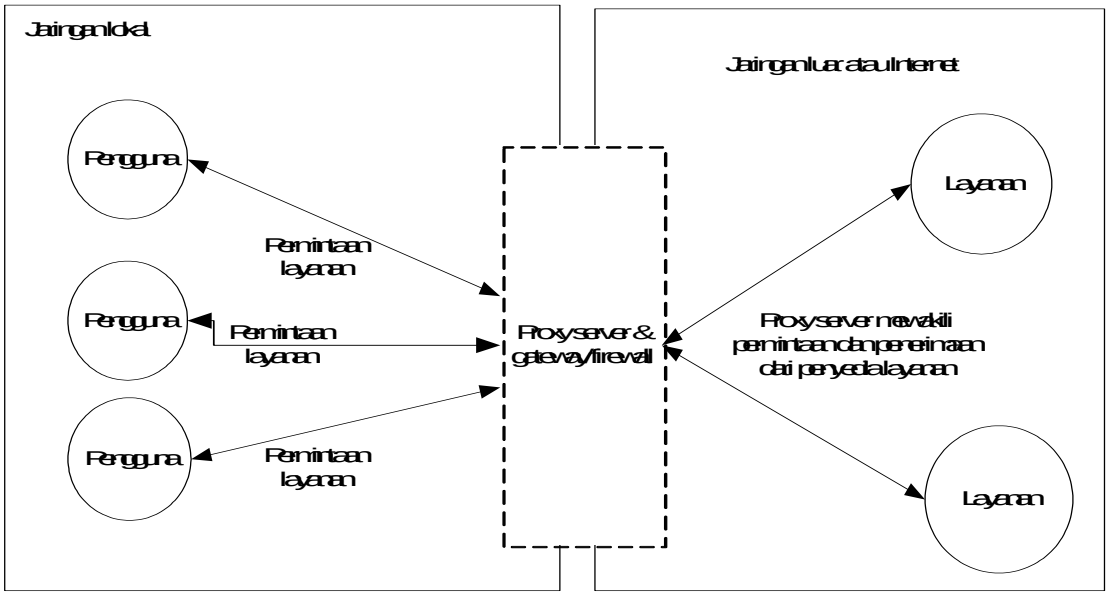
Proxy dapat dipahami sebagai pihak ketiga yang berdiri ditengah-tengah antara kedua pihak yang saling berhubungan dan berfungsi sebagai perantara, sedemikian sehingga pihak pertama dan pihak kedua tidak secara langsung berhubungan, akan tetapi masing-masing berhubungan dengan perantara, yaitu proxy.

Proxy dalam pengertiannya sebagai perantara, bekerja dalam berbagai jenis protokol komunikasi jaringan dan dapat berada pada level-level yang berbeda pada hirarki layer protokol komunikasi jaringan. Suatu perantara dapat saja bekerja pada layer Data-Link, layer Network dan Transport, maupun layer Aplikasi dalam hirarki layer komunikasi jaringan menurut OSI. Namun pengertian proxy server sebagian besar adalah untuk menunjuk suatu server yang bekerja sebagai proxy pada layer Aplikasi, meskipun juga akan dibahas mengenai proxy pada level sirkuit.

Dalam suatu jaringan lokal yang terhubung ke jaringan lain atau internet, pengguna tidak langsung berhubungan dengan jaringan luar atau internet, tetapi harus melewati suatu gateway, yang bertindak sebagai batas antara jaringan lokal dan jaringan luar. Gateway ini sangat penting, karena jaringan lokal harus dapat dilindungi dengan baik dari bahaya yang mungkin berasal dari internet, dan hal tersebut akan sulit dilakukan bial tidak ada garis batas yang jelas jaringan lokal dan internet. Gateway juga bertindak sebagai titik dimana sejumlah koneksi dari pengguna lokal akan

terhubung kepadanya, dan suatu koneksi ke jaringan luar juga terhubung kepadanya. Dengan demikian, koneksi dari jaringan lokal ke internet akan menggunakan sambungan yang dimiliki oleh gateway secara bersama-sama (connection sharing). Dalam hal ini, gateway adalah juga sebagai proxy server, karena menyediakan layanan sebagai perantara antara jaringan lokal dan jaringan luar atau internet.

Diagram berikut menggambarkan posisi dan fungsi dari proxy server, diantara pengguna dan penyedia layanan:



Gambar 2.4 Fungsi Proxy Server

2.2.7 Transparent Proxy

Salah satu kompleksitas dari proxy pada level aplikasi adalah bahwa pada sisi pengguna harus dilakukan konfigurasi yang spesifik untuk suatu proxy tertentu agar bisa menggunakan layanan dari suatu proxy server. Bila diinginkan agar pengguna tidak harus melakukan konfigurasi khusus, kita

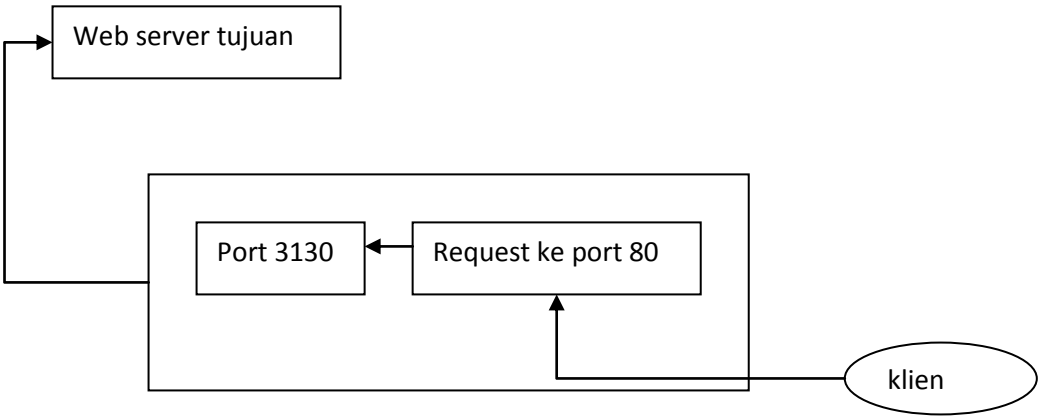
bisa mengkonfigurasi proxy/cache server agar berjalan secara benar-benar transparan terhadap pengguna (transparent proxy). Biasanya cara ini memerlukan bantuan dan konfigurasi aplikasi firewall (yang bekerja pada layer network) untuk bisa membuat transparent proxy yang bekerja pada layer aplikasi.

Transparent proxy dapat berguna untuk "memaksa pengguna" menggunakan proxy/cache server, karena pengguna benar-benar tidak mengetahui tentang keberadaan proxy ini, dan apapun konfigurasi pada sisi pengguna, selama proxy server ini berada pada jalur jaringan yang pasti dilalui oleh pengguna untuk menuju ke internet, maka pengguna pasti dengan sendirinya akan "menggunakan" proxy/cache ini.

Cara membuat transparent proxy adalah dengan membelokkan arah (redirecting) dari paket-paket untuk suatu aplikasi tertentu, dengan menggunakan satu atau lebih aturan pada firewall/router. Hal ini bisa dilakukan karena setiap aplikasi berbasis TCP akan menggunakan salah satu port yang tersedia, dan firewall dapat diatur agar membelokkan paket yang menuju ke port layanan tertentu, ke arah port dari proxy yang bersesuaian.

Sebagai contoh, pada saat klient membuka hubungan HTTP (port 80) dengan suatu web server, firewall pada router yang menerima segera mengenali bahwa ada paket data yang berasal dari klien dengan nomor port 80. Disini kita juga mempunyai satu HTTP proxy server yang berjalan pada port 3130. Maka pada firewall router kita buat satu aturan yang menyatakan bahwa setiap paket yang datang dari jaringan lokal menuju ke port 80 harus

dibelokkan ke arah alamat HTTP proxy server port 3130. Akibatnya, semua permintaan web dari pengguna akan masuk dan diwakili oleh HTTP proxy server diatas.



Gambar 2.5 Skema Proses Transparent Proxy

Jadi secara umum keuntungan dari metode transparent proxy itu sendiri adalah :

1. Kemudahan administrasi jaringan, dengan artian browser yang digunakan klien tidak harus dikonfigurasi secara khusus yang menyatakan bahwa mereka menggunakan fasilitas proxy yang bersangkutan.
2. Sentralisasi kontrol, dengan artian, pergantian metode bypass proxy maupun penggunaan proxy oleh klien dapat dilakukan secara terpusat.

2.2.8 Proxy Server pada Level Sirkuit

Proxy server yang bekerja pada level sirkuit dibuat untuk menyederhanakan keadaan. Proxy ini tidak bekerja pada layer aplikasi, akan tetapi bekerja sebagai “sambungan” antara layer aplikasi dan layer transport, melakukan pemantauan terhadap sesi-sesi TCP antara pengguna dan penyedia layanan atau sebaliknya. Proxy ini juga masih bertindak sebagai perantara, namun juga membangun suatu sirkuit virtual diantara layer aplikasi dan layer transport.

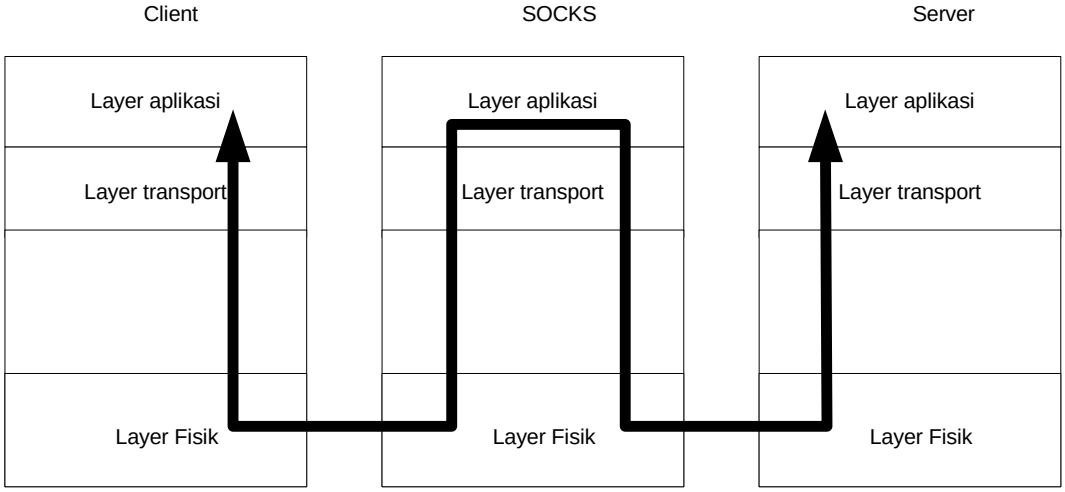
Dengan proxy level sirkuit, aplikasi klien pada pengguna tidak perlu dikonfigurasi untuk setiap jenis aplikasi. Sebagai contoh, dengan menggunakan Microsoft Proxy Server, sekali saja diperlukan untuk menginstall WinSock Proxy pada komputer pengguna, setelah itu aplikasi-apliakasi seperrti Windows Media Player, IRC atau telnet dapat langsung menggunakannya seperti bila terhubung langsung lke internet.

Kelemahan dari proxy level sirkuit adalah tidak bisa memeriksa isi dari paket yang dikirimkan atau diterima oleh aplikasi-aplikasi yang menggunakannya. Kelemahan ini dicoba diatasi menggunakan teknologi yang disebut SOCKS. SOCKS adalah proxy level sirkuit yang dapat digunakan untuk semua aplikasi (generik proxy) yang berbasis TCP/IP, dikembangkan sekitar tahun 1990 oleh Internet Engineering Task Force (IETF) dan sudah mencapai versi 5 (RFC 1928). SOCKS menyediakan standar yang independen dari platform yang digunakan untuk mengakses proxy level sirkuit. Salah satu kemampuan penting SOCKS versi 5 adalah

tambahan proses autentikasi dan password, serta memberikan layanan proxy terhadap layanan berbasis UDP, dengan pertama-tama melakukan koneksi TCP, den kemudian menggunakannya untuk relay bagi data UDP.

SOCKS terdiri dari dua komponen, yaitu SOCKS server dan SOCKS klien. SOCKS server diimplementasikan pada leyer aplikasi, sedangkan SOCKS klien diimplementasikan diantara layer aplikasi dan layer transport. Kegunaan pokoknya adalah untuk bisa menyelenggarakan koneksi dari satu host pada satu sisi dari SOCKS server dengan host lain pada sisi yang lain dari SOCKS server, tanpa kedua host harus terhubung langsung dalam konteks TCP/IP.

Diagram berikut menggambarkan posisi SOCKS:



Gambar 2.6 Posisi SOCKS

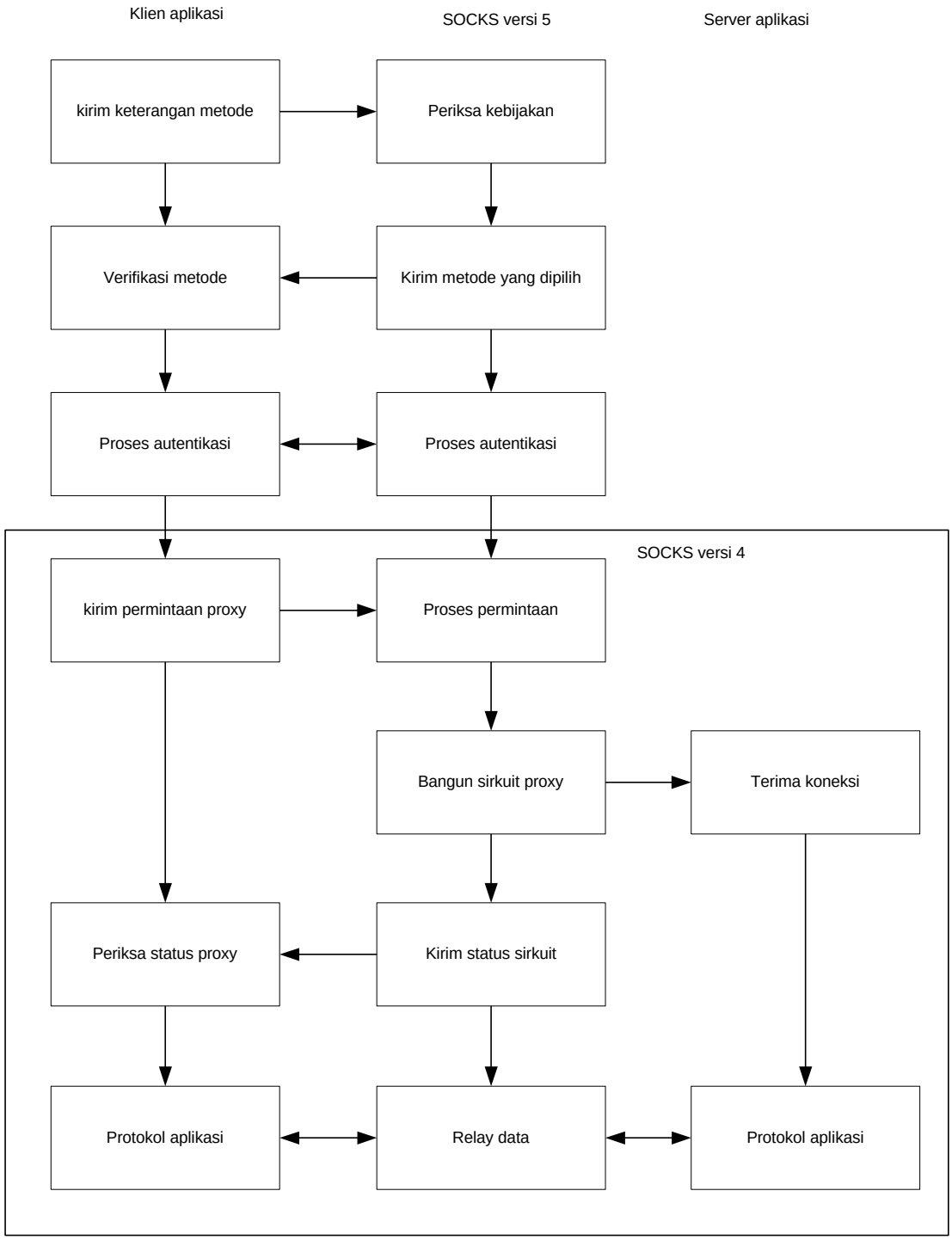
Ketika satu aplikasi klien ingin terhubung dengan server aplikasi, pertama-tama dia menghubungi SOCKS proxy server. Proxy inilah yang akan melakukan relay data dan menghubungkan klien dengan server. Bagi si klien, SOCKS proxy server adalah server, dan bagi server, SOCKS proxy server adalah klien. SOCKS proxy

melakukan 3 tahap proses yaitu membuat permintaan koneksi, membuat sirkuit proxy-nya, dan melakukan relay data. SOCKS versi 5 menambah satu prosedur yaitu proses autentikasi pada setiap langkah diatas.

Aplikasi yang menggunakan SOCKS versi 5 sejumlah mempunyai keunggulan yaitu :

1. Proxy generik yang tidak tergantung pada aplikasinya (application-independent proxy). SOCKS membuat dan mengatur channel komunikasi yang digunakan untuk semua aplikasi jaringan. Adanya aplikasi baru tidak memerlukan pengembangan tambahan. Proxy layer aplikasi harus membuat software proxy baru untuk setiap aplikasi baru, dan proxy layer network dengan inspeksi penuh harus membuat cara inspeksi protokol baru.
2. akses yang transparan pada jaringan dengan banyak server proxy.
3. kemudahan autentikasi dan metode enkripsi. Hanya menggunakan satu protokol saja untuk pembangunan channel komunikasi semua pengguna dan aplikasi, dan proses autentikasinya. Kebanyakan protokol tuneling memisahkan proses autentikasi dan proses pembangunan channel komunikasi.
4. kemudahan membangun aplikasi jaringan tanpa harus membuat proxy-nya.
5. manajemen kebijakan yang sederhana atas keamanan jaringan.

Diagram berikut menggambarkan aliran kendali model aliran kendali SOCKSv5:

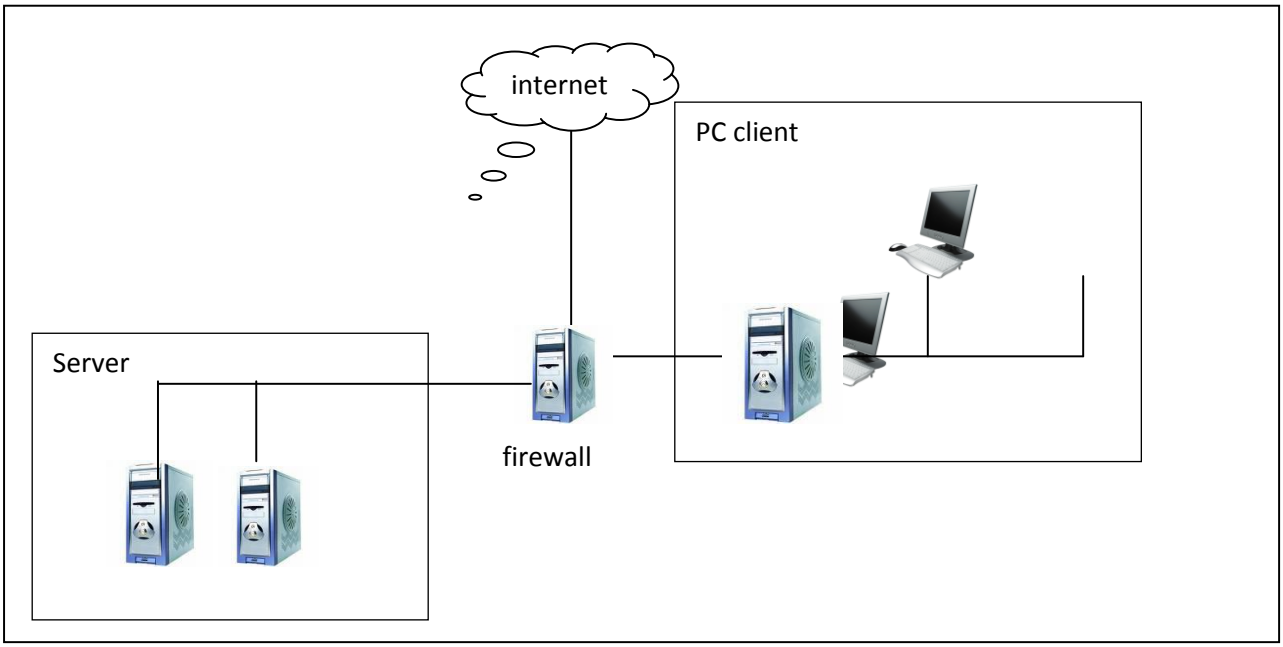


Gambar 2.7 Aliran Kendali SOCKSv5

2.2.9 Firewall

Secara definisi *firewall* adalah sebuah sistem atau sekelompok sistem yang menerapkan sebuah *access control policy* terhadap lalu lintas jaringan yang melewati titik-titik akses jaringan. Sehingga dapat disimpulkan *firewall* bertanggung jawab untuk menolak atau memberi akses kepada lalu lintas data di level jaringan antara internet dan sistem organisasi.

Proxy server juga biasanya menjadi satu dengan firewall server, meskipun keduanya bekerja pada layer yang berbeda. Firewall atau packet filtering yang digunakan untuk melindungi jaringan lokal dari serangan atau gangguan yang berasal dari jaringan internet bekerja pada layer network, sedangkan proxy server bekerja pada layer aplikasi. Firewall biasanya diletakkan pada router-router, untuk sehingga bisa melakukan filtering atas paket yang lewat dari dan ke jaringan-jaringan yang dihubungkan.



Gambar 2.8 Implementasi *Firewall* Tunggal

2.2.10 IPCOP

IPCOP adalah suatu distribusi Linux yang menyediakan fitur simple-to-manage firewall appliance berbasis perangkat keras PC. IPCOP juga merupakan suatu stateful firewall dibuat berdasarkan pada Linux netfilter framework.

Distro ini awalnya dikembangkan oleh tim yang mengembangkan Smoothwall Linux firewall, perkembangan selanjutnya, proyek IPCop dikembangkan dengan bebas, dan saat ini sudah terpisah sepenuhnya.

IPCOP dikembangkan secara Opensource, dengan komunitas pengembang independent yang tersebar diseuluruh dunia. CD-ROM image untuk instalasi dapat dengan mudah di download dan memiliki miror yang cukup banyak.

Pengembangan IPcop terus berlanjut hingga saat ini sudah mencapai seri rilis 1.4.x. Sekarang sudah dirilis versi 1.4.21 dibulan July 2008. saat ini sedang dikembangkan IPcop Version 2.0.

Walaupun bukan bagian dari komunitas resmi, banyak sekali yang memberikan kontribusi bagi pengembangan IPcop. Pada umumnya mereka membuat modul-modul tambahan yang di kenal sebagai Add-ons. Addons ini memberikan tambahan kemampuan IPCop menjadi lebih handal, beberapa addons yang paling sering digunakan adalah QoS untuk bandwidth management, Advanced Proxy dan Url Filter untuk proxy dan filter akses, E-mail Virus scanner, OpenVPN, dan banyak lagi. Akan kita bahas mengenai addons ini secara terpisah.

"*The Bad Packet Stop Here*" merupakan slogan yang diusung untuk menjadikan IPCop sebagai firewall yang handal.

2.2.10.1 Konfigurasi IPCOP

Network Interface

Network interface IPCop terdefinisi atas empat macam yaitu RED, GREEN, BLUE dan ORANGE.

1. RED Network Interface

   Network ini adalah interface internet atau untrusted network. Pada dasarnya yang dilindungi oleh IPCop adalah network GREEN, BLUE dan ORANGE dari traffic yang berasal dari network RED.

2. GREEN Network Interface

   Interface ini hanya terhubung ke komputer yang dilindungi oleh IPCop. Atau lebih dikenal dengan istilah local network. Traffic ke interface ini diarahkan lewat LAN card yang terpasang di IPCop firewall.

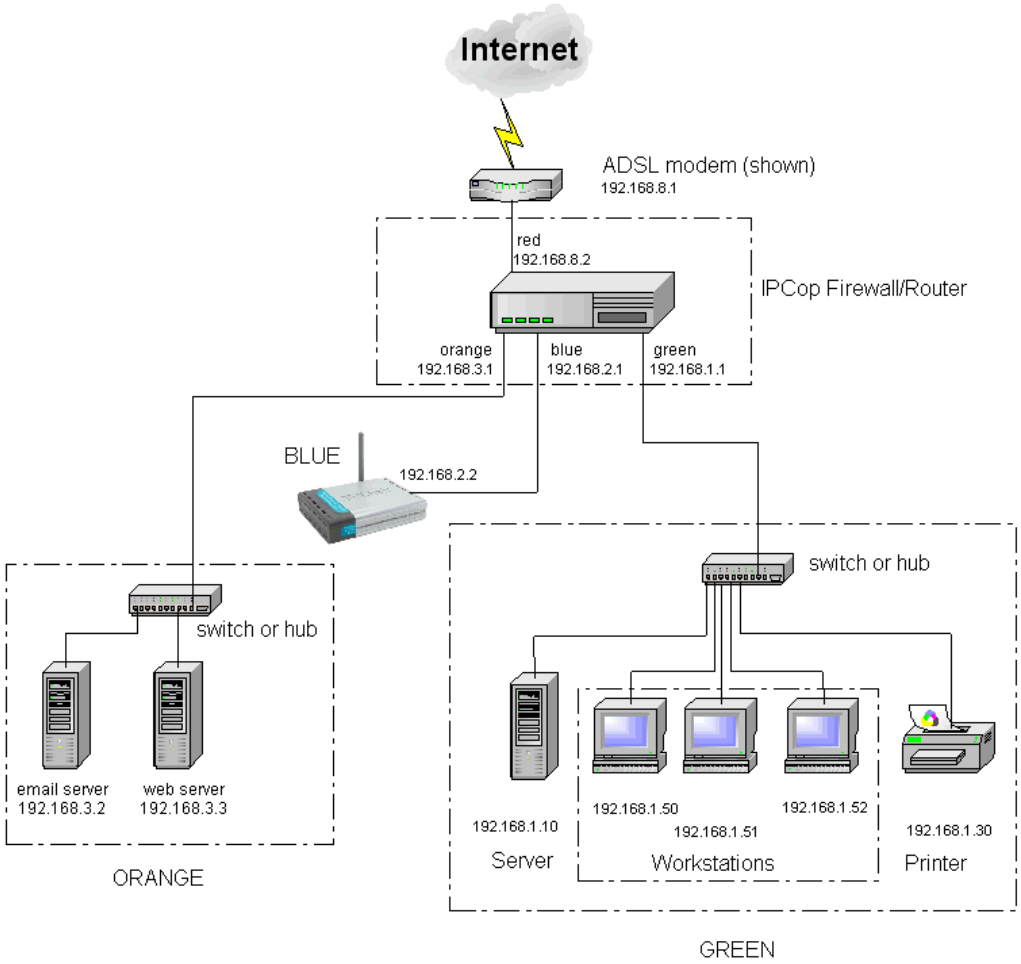
3. BLUE Network Interface

   Interface ini adalah interface pilihan (digunakan jika dibutuhkan) yang dapat digunakan untuk koneksi perangkat wireless di network yang berbeda dari local network. Komputer dibawah interface ini tidak dapat terhubung dengan komputer yang berada di interface GREEN kecuali dikontrol menggunakan ‘pinholes’ atau via koneksi VPN. Traffic ke interface ini juga

diarahkan lewat LAN card yang terpasang di IPCop firewall.

4. ORANGE Network Interface

Interface ini juga merupakan interface pilihan yang digunakan untuk menempatkan server yang boleh diakses oleh network yang berbeda. Komputer dibawah interface ini tidak dapat terhubung dengan komputer yang berada di interface GREEN atau BLUE kecuali dikontrol menggunakan 'DMZ pinholes'. Traffic ke interface ini juga diarahkan lewat LAN card yang terpasang di IPCop firewall.



Gambar 2.9 Konfigurasi RED, ORANGE, BLUE, GREEN