BAB II

TINJAUAN PUSTAKA

2.1 Profil Layanan Pengadaan Secara Elektronik (LPSE)

2.1.1 Sejarah Layanan Pengadaan Secara Elektronik (LPSE)

Tentang LPSE

Pengadaan barang dan jasa dapat didefinisikan sebagai pengadaan atau pemasokan barang, layanan jasa pekerjaan bangunan atau konstruksi atau pekerjaan fisik lainnya atau konsultansi atas hal tertentu dengan suatu spesifikasi fisik yang ditetapkan pengguna barang atau jasa dan dalam pelaksanaanya diawasi oleh pengguna barang atau jasa tersebut

LPSE Regional/Departemen

Untuk memperluas akses *e-procurement* ke seluruh instansi pemerintah, LKPP memberi kesempatan kepada departemen, kementerian, LPND (Lembaga Pemerintah Non Departemen) pemerintah provinsi, kabupaten, kota, dan instansi pemerintah lainnya untuk mendirikan LPSE di instansi masing-masing. LPSE-LPSE ini memiliki fungsi seperti LPSE Nasional namun melayani instansi masing-masing. Dalam pendirian LPSE Regional/Departemen, LKPP akan memberikan bimbingan, petunjuk teknis, pelatihan, dan Aplikasi LPSE.

LKPP

LKPP atau Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah adalah lembaga yang dibentuk oleh pemerintah dengan Keppres 106/2007. Lembaga ini merupakan perluasan Pusat Pengembangan Kebijakan Pengadaan Barang/Jasa Publik - Bappenas.

Aplikasi LPSE

Aplikasi LPSE merupakan aplikasi *e-procurement* yang dikembangkan oleh LKPP. Pada menu atau modul dalam aplikasi LPSE terdapat sejumlah fungsi-fungsi proses pelelangan dan transaksi pengadaan barang dan jasa yang bersifat umum, seperti registrasi peserta, daftar barang dan jasa yang ditenderkan, penjelasan persyaratan lelang barang atau jasa beserta harganya, pengisian proposal, mekanisme negosiasi dan penyanggahan, lelang *on line*, transaksi/ *purchase order*, form serah terima dan database para penyedia.

Secara nasional, pengembangan dan perumusan kebijakan pengadaan barang/jasa pemerintah dilaksanakan oleh Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah (**LKPP**) yang merupakan lembaga pemerintah non departemen yang berada di bawah dan bertanggung jawab kepada Presiden. Lembaga yang dibentuk berdasarkan Perpres No 106 tahun 2007 ini merupakan perluasan Pusat Pengembangan Kebijakan Pengadaan Barang/Jasa Publik – Bappenas.

Hasil evaluasi LKPP berdasarkan pengalaman sejak tahun 2004 dalam hal pemberlakuan Keppres No. 80 Tahun 2003 menunjukkan, efisiensi akan akan tercapai apabila proses pengadaan barang/jasa berlangsung secara transparan dan diikuti oleh sejumlah peserta pengadaan yang cukup banyak serta mengedepankan proses persaingan yang sehat.

Layanan Pengadaan Secara Elektronik (LPSE) merupakan pengadaan barang/jasa secara elektronik dengan menggunakan teknologi informasi dan komunikasi berbasis internet (*e-procurement*) yang memfasilitasi lelang secara cepat, transparan, mudah, akurat dan terlindungi.

Pada dasarnya lelang pengadaan barang/jasa secara elektronik tidak berbeda dengan penyelenggaraan lelang secara manual yang mengacu kepada Keputusan Presiden RI No. 80 Tahun 2003 tentang Pedoman pelaksanaan Pengadaan barang / Jasa Pemerintah beserta aturan-aturan perubahannya, terakhir sebagaimana yang diatur dalam Peraturan Presiden No. 8 Tahun 2006.

Penyelenggaraan pengadaan barang dan jasa pemerintah secara elektronik mempunyai landasan hukum yang kuat dan menjamin keabsahaannya. Peraturan perundang-undang tersebut antara lain :

1. Keputusan Presiden Nomor 80 Tahun 2003 tentang Pedoman Pelaksanaan Pengadaan Barang dan Jasa Publik;
2. Instruksi Presiden Nomor 5 Tahun 2003 tentang Paket Kebijakan Ekonomi Menjelang dan Sesudah Berakhirnya Program Kerjasama dengan International Monetary Fund (IMF);
3. Instruksi Presiden Nomor 5 Tahun 2004 tentang Percepatan Pemberantasan Korupsi;
4. Peraturan Presiden Nomor 8 Tahun 2006 tentang Perubahan Keempat atas Keputusan Presiden Nomor 8 Tahun 2003 (tentang Pedoman Pelaksanaan Pengadaan Barang dan Jada Pemerintah).
5. Undang Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Aplikasi LPSE merupakan aplikasi *e-procurement* yang dikembangkan oleh LKPP. Pada menu atau modul dalam aplikasi LPSE terdapat sejumlah fungsi-fungsi proses pelelangan dan transaksi pengadaan barang dan jasa yang bersifat umum, seperti registrasi peserta, daftar barang dan jasa yang ditenderkan,

penjelasan persyaratan lelang barang atau jasa beserta harganya, pengisian proposal, mekanisme negosiasi dan penyanggahan, lelang *on line*, transaksi/ *purchase order*, form serah terima dan database para penyedia.

Salah satu unsur penting dalam *e-procurement* adalah pertukaran dokumen. Untuk menjamin keamanan dokumen penawaran rekanan, LKPP bekerja sama dengan Lembaga Sandi Negara mengembangkan Aplikasi Pengaman Dokumen (Apendo) yang digunakan untuk melakukan enkripsi dan dekripsi dokumen

Guna memperluas akses *e-procurement* ke seluruh instansi dan jenjang pemerintahan, LKPP memberi kesempatan, antara lain, kepada pemerintah provinsi, kabupaten dan kota untuk mendirikan LPSE di daerah masing-masing. LPSE-LPSE ini memiliki fungsi seperti LPSE Nasional, namun melayani daerah masing-masing. Dalam pendirian LPSE Regional, LKPP akan memberikan bimbingan, petunjuk teknis, pelatihan, dan Aplikasi LPSE. Aplikasi ini dikembangkan dengan semangat efisiensi nasional sehingga tidak memerlukan biaya apapun untuk lisensinya; baik lisensi Aplikasi LPSE itu sendiri maupun perangkat lunak pendukungnya.

Aplikasi yang ada pada LPSE Jawa Barat saat ini sudah mampu mendukung penyelenggaraan pengadaan barang, pengadaan jasa pemborongan konstruksi dan pengadaan jasa lainnya, melalui proses penilaian kompetensi secara prakualifikasi maupun pascakualifikasi dengan metode penyampaian dokumen satu sampul.

Berikut ini diuraikan beberapa terminologi dalam penyelenggaraan lelang dan pengadaan barang dan jasa umumnya sebagaimana yang diatur dalam Keputusan Presiden Nomor 80 Tahun 2003 beserta aturan-aturan perubahannya, serta layanan pengadaan barang dan jasa pemerintah daerah secara elektronik.

- **Publik** adalah perusahaan yang berminat untuk menjadi peserta lelang.
- **Agency** adalah Satuan Kerja Perangkat Daerah (SKPD) atau instasi pemerintah yang ikut dalam LPSE Regional.
- **Pengelola Sistem Informasi Layanan Pengadaan Secara Elektronik** yang selanjutnya disebut Pengelola LPSE adalah pengelola sistem informasi layanan pengadaan barang/jasa pemerintah secara elektronik.
- **Pengguna Anggaran** atau yang lazim disingkat PA, adalah pejabat pemegang kewenangan penggunaan anggaran untuk melaksanakan tugas pokok dan fungsi SKPD yang dipimpinnya.
- **Kuasa Pengguna Anggaran** atau yang lazim disingkat KPA, adalah pejabat yang diberi kuasa untuk melaksanakan sebagian kewenangan PA dalam melaksanakan sebagian tugas dan fungsi SKPD serta untuk menggunakan anggaran SKPD.
- **Pejabat Pembuat Komitmen** atau yang lazim disingkat PjPK, adalah pejabat yang diangkat oleh Kepala SKPD selaku PA sebagai pemilik pekerjaan yang bertanggung jawab atas pelaksanaan pengadaan barang/jasa.
- **Panitia Pengadaan** adalah tim yang diangkat oleh PA/KPA untuk melaksanakan pemilihan penyedia barang/jasa.
- **Unit Layanan Pengadaan** adalah unit yang terdiri dari pegawai-pegawai yang telah memiliki sertifikat keahlian pengadaan barang/jasa pemerintah, yang dibentuk oleh PA yang bertugas secara khusus untuk melaksanakan pemilihan penyedia barang/jasa di lingkungan pemerintah daerah.
- **Penyedia Barang/Jasa** atau ***Vendor*** adalah badan usaha atau orang perseorangan yang kegiatan usahanya menyediakan barang/jasa.

- **Registrasi** adalah proses pendaftaran penyedia barang/jasa untuk mendapatkan kode akses (*user id* dan *password*) ke dalam sistem aplikasi Layanan Pengadaan Secara Elektronik.
- **Verifikasi** adalah proses penentuan kelayakan penyedia barang/jasa oleh LPSE melalui mekanisme kontrol secara asas nyata dalam proses registrasi/pendaftaran calon penyedia barang/jasa yang meliputi persetujuan *password* dan penyampaian notifikasi persetujuan.
- **Verifikator**. adalah pejabat yang bertugas melakukan verifikasi .
- **Certificate Agent** adalah pejabat yang memberikan jaminan keamanan baik kepada rekanan maupun panitia. CA memberikan kepastikan kepada rekanan bahwa dokumen penawaran yang dikirimkannya tidak dapat dibuka oleh panitia sebelum tanggal yang ditentukan.
- **Tanda Tangan Elektronik** adalah tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan otentikasi.

Pada awal proses, PjPK membuat paket lelang yang dikirimkan kepada Panitia Pengadaan. Panitia kemudian melaksanakan lelang yang dimaksud dengan mengatur jadwal, kualifikasi dan lain-lain sebagainya. Kemudian hasil pekerjaan ini diajukan kembali guna mendapat persetujuan dari PjPK. Bila PjPK setuju, barulah lelang bisa diumumkan kepada publik dan kemudian bisa diikuti oleh para rekanan/*vendor*.

Untuk dapat mengikuti lelang pada tahap awal *vendor* harus melakukan verifikasi data perusahaan dengan terlebih dahulu mendaftar melalui akses internet pada situs LPSE Nasional atau Regional dengan mengisi formulir pendaftaran,

mengirimkan kepada sistem LPSE dengan meng-klik tombol daftar, men-*download* dokumen, mengikuti *aanwijzing* secara *chatting*, menyiapkan dokumen dalam bentuk digital dan meng-*upload*-nya ke situs LPSE.

Setelah itu Direktur Utama Perusahaan tersebut atau Kuasanya (dinyatakan secara tertulis) datang ke LPSE dengan membawa *print-out* formulir pendaftaran dilengkapi dengan data (bukti) asli seperti SIUP asli, KTP asli Direktur Utama, Akta Pendirian dan Akta Perubahan asli, dan lain-lain yang disyaratkan dalam formulir untuk dilakukan verifikasi oleh verifikator LPSE. Setelah datanya dicek kesahihannya, verifikator memasukkannya ke *database* LPSE dan kepada *vendor* yang bersangkutan diberikan *User ID* dan *password* untuk dipergunakan pada saat mengikuti lelang secara elektronik.

Vendor yang dapat mengikuti lelang secara elektronik yang difasilitasi oleh LPSE ialah *vendor* yang telah terdaftar pada *database* LPSE serta memiliki *User ID* dan *Password*.

Vendor dapat melihat secara *on-line* hasil evaluasi panitia, pengumuman pemenang, serta dapat melakukan sanggahan apabila menemukan hal-hal yang disyaratkan pada Pasal 27 Keppres No. 80 tahun 2003.

2.1.2 Logo Layanan Pengadaan Secara Elektronik (LPSE)



Gambar 2.1: Logo Pemprov Jabar

Secara keseluruhan lambang Pemerintah Propinsi Jawa Barat berbentuk bulat telur dengan hiasan pita di bagian bawahnya yang berisikan motto Jawa Barat. Makna daripada bentuk dan motif yang terdapat dalam lambang ialah :

1. **Bentuk bulat telur** pada lambang Jawa Barat berasal dari bentuk perisai yang banyak dipakai oleh para laskar kerajaan zaman dahulu, makna perisai sebagai penjagaan diri.
2. **Kujang** yang berada di tengah-tengah adalah senjata pusaka yang tajam serba guna bagi masyarakat Sunda masa lalu. Lima lubang pada kujang melambangkan dasar negara, Pancasila.
3. Setangkai **padi** yang terdapat di sisi sebelah kiri melambangkan bahan makanan pokok masyarakat Jawa Barat sekaligus juga melambangkan kesuburan pangan, dan jumlah padi 17 menggambarkan tanggal Proklamasi Republik Indonesia.
4. **Kapas** yang berada di sebelah kanan melambangkan kesuburan sandang, dan 8 kuntum bunga menggambarkan bulan proklamasi Republik Indonesia.
5. **Gunung** yang terdapat di bawah padi dan kapas melambangkan bahwa daerah Jawa Barat terdiri atas daerah pegunungan.

6. **Sungai** dan **terusan** yang terdapat di bawah gunung sebelah kiri melambangkan di Jawa Barat banyak terdapat sungai dan saluran air yang sangat berguna untuk pertanian.
7. **Petak-petak** yang terdapat di bawah gunung sebelah kanan melambangkan banyaknya pesawahan dan perkebunan. Masyarakat Jawa Barat umumnya hidup mengandalkan kesuburan tanahnya yang diolah menjadi lahan pertanian.
8. **Dam/bendungan** yang terdapat di tengah-tengah bagian bawah antara gambar sungai dan petak, melambangkan kegiatan di bidang irigasi yang merupakan salah satu perhatian pokok mengingat Jawa Barat merupakan daerah agraris.

MAKNA WARNA

Warna yang mendominasi pada lambang Jawa Barat adalah hijau, makna warna-warna yang dipergunakan dalam mewarnai motif lambang adalah :

1. Hijau bermakna kesuburan dan kemakmuran tanah Jawa Barat.
2. Kuning bermakna keagungan, kemulyaan dan kekayaan.
3. Hitam bermakna keteguhan dan keabadian.
4. Biru bermakna ketentraman atau kedamaian
5. Merah bermakna keberanian.
6. Putih bermakna kemurnian /kesucian atau kejujuran.

MOTTO DAERAH

Motto daerah Jawa Barat adalah ***"Gemah Ripah Repeh Rapih"***, kata gemah-ripah dan repeh-rapih merupakan kata majemuk yang mempunyai arti sebagai berikut :

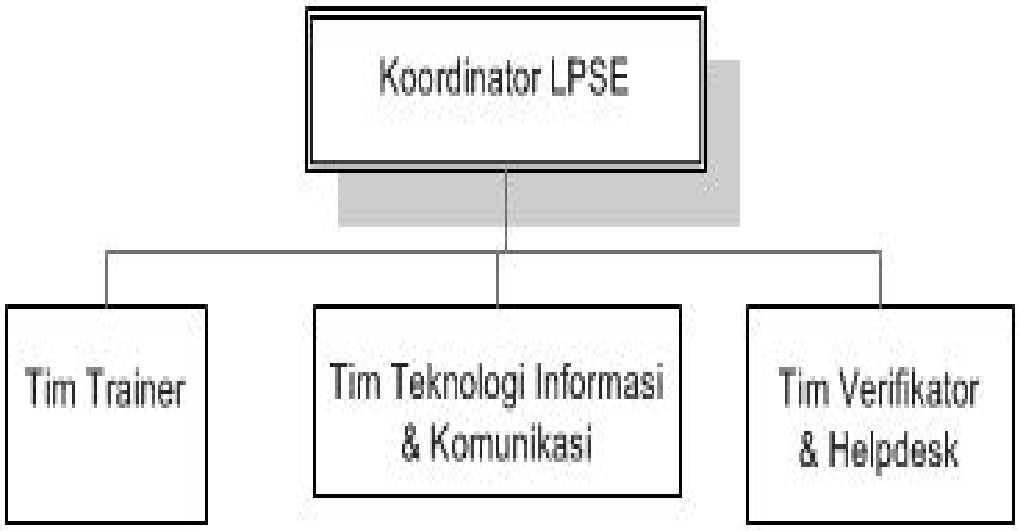
1. **Gemah-ripah** : subur makmur, cukup sandang dan pangan.
2. **Repeh-rapih** : rukun dan damai atau aman sentosa.

Arti dari motto daerah Jawa Barat secara keseluruhan ialah menyatakan bahwa Jawa Barat merupakan daerah yang kaya raya/subur makmur didiami oleh banyak penduduk yang hidup rukun dan damai.

2.1.3 Badan Hukum Layanan Pengadaan Secara Elektronik (LPSE)

LPSE (Layanan Pengadaan Secara Elektronik) merupakan instansi pemerintah yang dibawah naungan DISKOMINFO.

2.1.4 Struktur Organisasi dan Job Description



Gambar 2.2: Struktur Organisasi

Menurut struktur organisasi di atas maka job descriptionnya adalah sebagai berikut :

1. Tim Trainer

   Pada instansi ini tim trainer bertugas sebagai pelatih dalam pelatihan penggadaian kepada suatu perusahaan yang belum mengerti cara penggadaian secara elektronik.

2. Tim Teknologi Informasi dan Komunikasi

Tim teknologi dan komunikasi bertugas sebagai penaggungjawab dalam penggadaian secara on-line.

3. Tim Verifikator dan Helpdesk

   Tim verifikator dan Helpdesk bertugas menerima pendaftaran peserta yang akan melakukan penggadaian secara elektronik dan juga menerima keluhan-keluhan peserta.

2.2 Landasan Teori

2.2.1 Pengenalan Jaringan Komputer

Jaringan berfungsi untuk mengatur hubungan antara pengirim dan penerima sedemikian rupa sehingga keduanya dapat saling berkomunikasi. Jaringan juga dibutuhkan untuk saling bertukar resource. Resource yang dimaksud adalah misalnya data, printer, file dan lain-lain.Network atau jaringan dalam bidang komputer dapat diartikan sebagai dua atau lebih komputer yang saling berhubungan sehingga dapat saling berkomunikasi dengan tujuan menimbulkan suatu efisiensi sentralisasi dan optimasi kerja.Bila dilihat dari sisi lingkupnya atau jangkauannya jaringan dapat dibagi menjadi beberapa jenis, yaitu :

- LAN (Local Area Network) : Hanya terdapat satu atau dua server dan ruang lingkupnya hanya terdapat dalam suatu lokasi atau gedung.
- WAN (Wide Area Network) : Merupakan gabungan dari LAN yang dimana ruang lingkupnya dapat saja satu lokasi, misalnya gedung bertingkat, atau dapat tersebar di beberapa lokasi di seluruh dunia, jaringan jenis ini membutuhkan minimal satu server untuk setiap LAN,

dan membutuhkan minimal dua server yang mempunyai lokasi berbeda untuk membentuknya.

- Internet : merupakan sekumpulan jaringan yang tersebar di seluruh dunia yang saling terhubung satu sama lain sehingga akan membentuk suatu jaringan. Komputer yang sangat besar. Layanan yang diberikan dalam jaringan ini antara lain : FTP, E-Mail, Chat, Telnet dll. Biasanya jaringan internet menggunakan protocol TCP/IP meskipun ada beberapa protocol lain yang bisa digunakan, misalnya : IPX Novel Netware, NetBios dan lain-lain.
- Intranet : Jaringan seperti ini merupakan gabungan antara dari LAN/WAN dengan internet. Jaringan ini memberikan layanan internet kepada terminal clientnya. Perbedaan mencolok antara Intranet dan Internet adalah Intranet melayani satu organisasi tertentu saja.

2.2.2.Firewall

Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri. Tujuan dari penggunaan firewall adalah untuk melindungi dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah workstation, server, router, atau local area network (LAN). Secara sederhana, konfigurasi firewall adalah sebagai berikut :

pc <==> ***firewall*** <==> **internet**

Pertama kali, Firewall untuk komputer dilakukan dengan menggunakan prinsip “non-routing” pada sebuah Unix host yang menggunakan 2 buah network interface card, network interface card yang pertama di hubungkan ke internet (jaringan lain) sedangkan yang lainnya dihubungkan ke pc (dengan catatan tidak terjadi “route” antara kedua network interface card di pc ini). Untuk dapat terkoneksi dengan Internet, harus memasuki server firewall (bisa secara remote, atau langsung), kemudian menggunakan resource yang ada pada komputer ini untuk berhubungan dengan Internet(jaringan lain) dan jika perlu menyimpan file/data, maka file tersebut dapat disimpan sementara di pc firewall anda baru kemudian mengkopikannya ke pc. Sehingga, internet tidak dapat berhubungan langsung dengan pc. Metode semacam ini masih banyak mempunyai kekurangan sehingga dikembangkan berbagai bentuk, konfigurasi dan jenis firewall dengan berbagai aturan di dalamnya. Firewall secara umum di peruntukkan untuk melayani :

1. Mesin/Komputer

   Setiap mesin/komputer yang terhubung langsung ke jaringan luar atau internet dan menginginkan semua yang terdapat pada komputernya terlindungi.

2. Jaringan

   Jaringan komputer yang terdiri lebih dari satu buah komputer dan berbagai jenis topologi jaringan yang digunakan, baik yang di miliki oleh perusahaan, organisasi dan sebagainya.

2.2.2.1 Karakteristik sebuah firewall

Secara umum, karakteristik sebuah firewall dapat dijelaskan sebagai berikut :

1. Seluruh hubungan/kegiatan dari dalam ke luar , harus melewati firewall. Hal ini dapat dilakukan dengan cara memblok/membatasi semua akses terhadap jaringan lokal, kecuali jika melewati firewall. Banyak bentuk jaringan yang memungkinkan agar konfigurasi ini terwujud.
2. Hanya kegiatan yang terdaftar/dikenal yang dapat melewati/melakukan hubungan, hal ini dapat dilakukan dengan mengatur policy pada konfigurasi keamanan lokal.
3. Firewall sendiri haruslah kebal atau relatif kuat terhadap serangan/kelemahan. Hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan sistem yang relatif aman.

2.2.2.2 Teknik yang digunakan oleh sebuah firewall

1. Service control (kendali terhadap layanan)

   Berdasarkan tipe-tipe layanan yang digunakan di Internet dan boleh diakses baik untuk kedalam ataupun keluar firewall. Biasanya firewall akan mencek no IP Address dan juga nomor port yang di gunakan baik pada protokol TCP dan UDP, bahkan bisa dilengkapi software untuk proxy yang akan menerima dan menterjemahkan setiap permintaan akan suatu layanan sebelum mengijinkannya.

2. Direction Conrol (kendali terhadap arah)

   Berdasarkan arah dari berbagai permintaan (request) terhadap layanan yang akan dikenali dan diijinkan melewati firewall.

3. User control (kendali terhadap pengguna)

Berdasarkan pengguna/user untuk dapat menjalankan suatu layanan, artinya ada user yang dapat dan ada yang tidak dapat menjalankan suatu servis,hal ini di karenakan user tersebut tidak di ijinkan untuk melewati firewall. Biasanya digunakan untuk membatasi user dari jaringan lokal untuk mengakses keluar, tetapi bisa juga diterapkan untuk membatasi terhadap pengguna dari luar.

4. Behavior Control (kendali terhadap perlakuan)

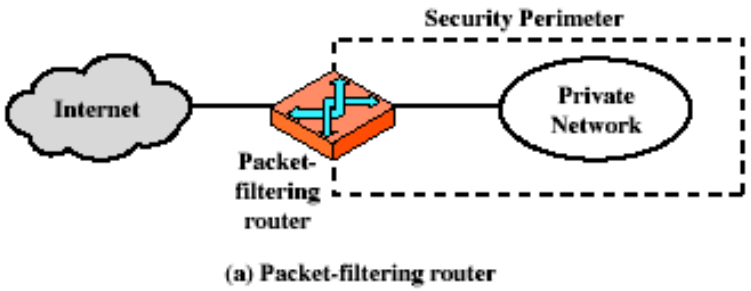
Berdasarkan seberapa banyak layanan itu telah digunakan. Misalnya, firewall dapat memfilter email untuk menanggulangi/mencegah spam.

2.2.2.3 Tipe-Tipe Firewall

1. Packet Filtering Router

Packet Filtering diaplikasikan dengan cara mengatur semua packet IP baik yang menuju, melewati atau akan dituju oleh packet tersebut. Pada tipe ini packet tersebut akan diatur apakah akan di terima dan diteruskan atau di tolak. Penyaringan packet ini di konfigurasikan untuk menyaring packet yang akan ditransfer secara dua arah (baik dari dan ke jaringan lokal). Aturan penyaringan didasarkan pada header IP dan transport header, termasuk juga alamat awal (IP) dan alamat tujuan (IP), protokol transport yang digunakan (UDP,TCP), serta nomor port yang digunakan. Kelebihan dari tipe ini adalah mudah untuk diimplementasikan, transparan untuk pemakai, relatif lebih cepat. Adapun kelemahannya adalah cukup rumitnya untuk menyetting paket yang akan difilter secara tepat, serta lemah dalam hal otentifikasi. Adapun serangan yang dapat terjadi pada firewall dengan tipe ini adalah:

- IP address spoofing : Intruder (penyusup) dari luar dapat melakukan ini dengan cara menyertakan/menggunakan ip address jaringan lokal yang telah diijinkan untuk melalui firewall.
- Source routing attacks : Tipe ini tidak menganalisa informasi routing sumber IP, sehingga memungkinkan untuk membypass firewall.
- Tiny Fragment attacks : Intruder membagi IP kedalam bagian-bagian (fragment) yang lebih kecil dan memaksa terbaginya informasi mengenai TCP header. Serangan jenis ini di design untuk menipu aturan penyaringan yang bergantung kepada informasi dari TCP header. Penyerang berharap hanya bagian (fragment) pertama saja yang akan di periksa dan sisanya akan bisa lewat dengan bebas. Hal ini dapat di tanggulangi dengan cara menolak semua packet dengan protokol TCP dan memiliki Offset = 1 pada IP fragment (bagian IP).

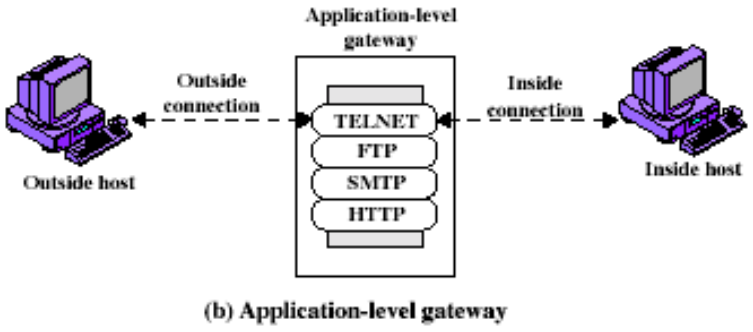


Gambar 2.3 Packet-Filtering Router

2. Application-Level Gateway

Application-level Gateway yang biasa juga di kenal sebagai proxy server yang berfungsi untuk memperkuat/menyalurkan arus aplikasi. Tipe ini akan mengatur semua hubungan yang menggunakan layer aplikasi ,baik itu FTP, HTTP, GOPHER dll. Cara kerjanya adalah apabila ada pengguna yang

menggunakan salah satu aplikasi semisal FTP untuk mengakses secara remote, maka gateway akan meminta user memasukkan alamat remote host yang akan di akses. Saat pengguna mengirimkan user ID serta informasi lainnya yang sesuai maka gateway akan melakukan hubungan terhadap aplikasi tersebut yang terdapat pada remote host, dan menyalurkan data diantara kedua titik. apabila data tersebut tidak sesuai maka firewall tidak akan meneruskan data tersebut atau menolaknya. Lebih jauh lagi, pada tipe ini Firewall dapat di konfigurasikan untuk hanya mendukung beberapa aplikasi saja dan menolak aplikasi lainnya untuk melewati firewall. Kelebihannya adalah relatif lebih aman daripada tipe packet filtering router lebih mudah untuk memeriksa (audit) dan mendata (log) semua aliran data yang masuk pada level aplikasi. Kekurangannya adalah pemrosesan tambahan yang berlebih pada setiap hubungan. yang akan mengakibatkan terdapat dua buah sambungan koneksi antara pemakai dan gateway, dimana gateway akan memeriksa dan meneruskan semua arus dari dua arah.

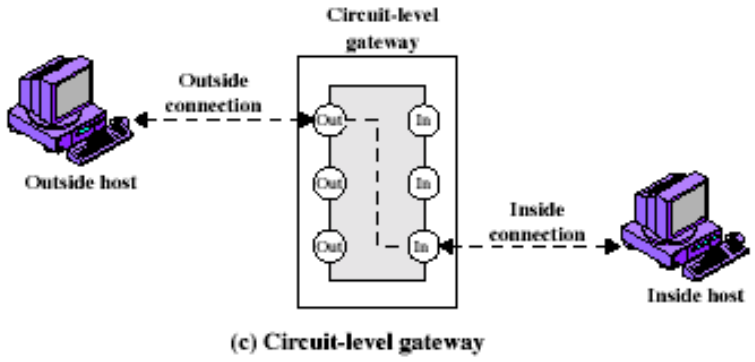


Gambar 2.4 Aplication-Level Gateway

3. Circuit-level Gateway

Tipe ketiga ini dapat merupakan sistem yang berdiri sendiri , atau juga dapat

merupakan fungsi khusus yang terbentuk dari tipe application-level gateway.tipe ini tidak mengijinkan koneksi TCP end to end (langsung) Cara kerjanya : Gateway akan mengatur kedua hubungan tcp tersebut, 1 antara dirinya (gw) dengan TCP pada pengguna lokal (inner host) serta 1 lagi antara dirinya (gw) dengan TCP pengguna luar (outside host). Saat dua buah hubungan terlaksana, gateway akan menyalurkan TCP segment dari satu hubungan ke lainnya tanpa memeriksa isinya. Fungsi pengamanannya terletak pada penentuan hubungan mana yang di ijinkan. Penggunaan tipe ini biasanya dikarenakan administrator percaya dengan pengguna internal (internal users).



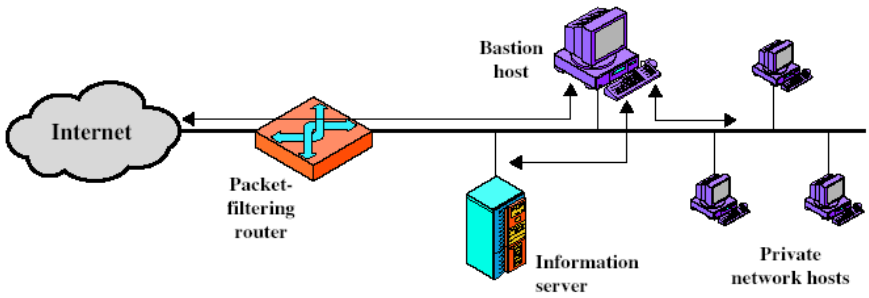
Gambar 2.5 Circuit-Level Gateway

2.2.2.4 Konfigurasi Firewall

1. Screened Host FIrewall system (single-homed bastion)

Pada konfigurasi ini, fungsi firewall akan dilakukan oleh packet filtering router dan bastion host*. Router ini dikonfigurasikan sedemikian sehingga untuk semua arus data dari Internet, hanya paket IP yang menuju bastion host yang di ijinkan. Sedangkan untuk arus data (traffic) dari jaringan internal, hanya paket IP dari bastion host yang di ijinkan untuk keluar. Konfigurasi ini mendukung

fleksibilitas dalam Akses internet secara langsung, sebagai contoh apabila terdapat web server pada jaringan ini maka dapat di konfigurasikan agar web server dapat diakses langsung dari internet. Bastion Host melakukan fungsi Authentikasi dan fungsi sebagai proxy. Konfigurasi ini memberikan tingkat keamanan yang lebih baik daripada packet-filtering router atau application-level gateway secara terpisah.

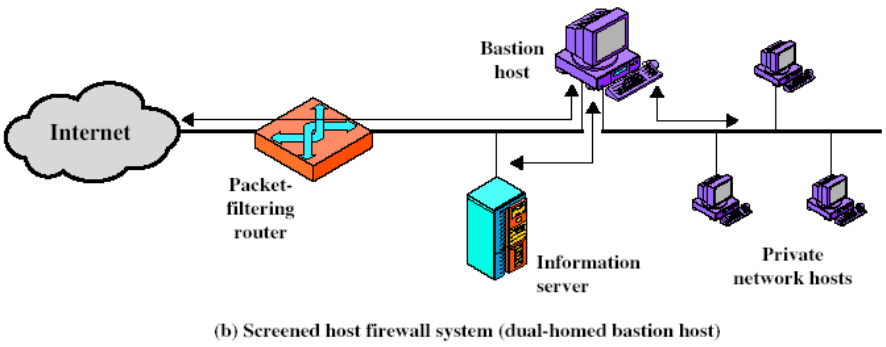


(a) Screened host firewall system (single-homed bastion host)

Gambar2.6 Screened Host Firewall System (Single-Homed Bastion Host)

2. Screened Host Firewall system (Dual-homed bastion)

Pada konfigurasi ini, secara fisik akan terdapat patahan/celah dalam jaringan. Kelebihannya adalah dengan adanya dua jalur yang meisahkan secara fisik maka akan lebih meningkatkan keamanan dibanding konfigurasi pertama,adapun untuk server-server yang memerlukan direct akses (akses langsung) maka dapat di letakkan ditempat/segmenrt yang langsung berhubungan dengan internet. Hal ini dapat dilakukan dengan cara menggunakan 2 buah NIC (network interface Card) pada bastion Host.

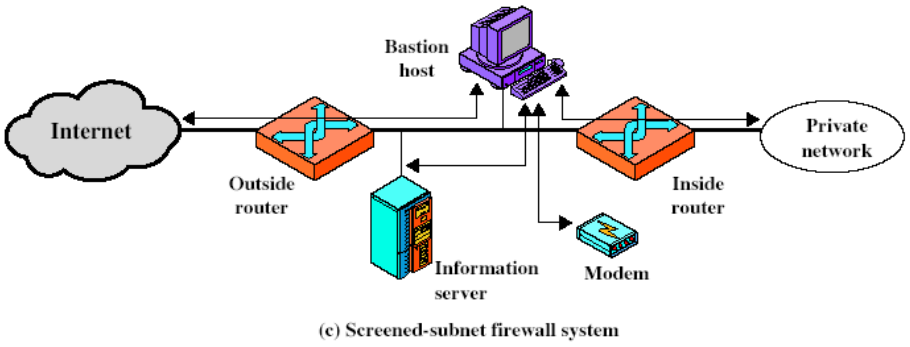


Gambar2.7 Screened Host Firewall System (Dual-Homed Host)

3. Screened subnet firewall

Ini merupakan konfigurasi yang paling tinggi tingkat keamanannya. kenapa? karena pada konfigurasi ini di gunakan 2 buah packet filtering router, 1 diantara internet dan bastion host, sedangkan 1 lagi diantara bastian host dan jaringan local konfigurasi ini membentuk subnet yang terisolasi. Adapun kelebihannya adalah :

- Terdapat 3 lapisan/tingkat pertahanan terhadap penyususp/intruder .
- Router luar hanya melayani hubungan antara internet dan bastion host sehingga jaringan lokal menjadi tak terlihat (invisible)
- Jaringan lokal tidak dapat mengkonstuksi routing langsung ke internet, atau dengan kata lain , Internet menjadi Invinsible (bukan berarti tidak bisa melakukan koneksi internet).



Gambar 2.8 Screened-Subnet Firewall System

2.2.2.5 Langkah-Langkah Membangun firewall

1. Mengidenftifikasi bentuk jaringan yang dimiliki

   Mengetahui bentuk jaringan yang dimiliki khususnya toplogi yang di gunakan serta protocol jaringan, akan memudahkan dalam mendesain sebuah firewall

2. Menentukan Policy atau kebijakan

   Penentuan Kebijakan atau Policy merupakan hal yang harus di lakukan, baik atau buruknya sebuah firewall yang di bangun sangat di tentukan oleh policy/kebijakan yang di terapkan. Diantaranya:

   - Menentukan apa saja yang perlu di layani. Artinya, apa saja yang akan dikenai policy atau kebijakan yang akan kita buat
   - Menentukan individu atau kelompok-kelompok yang akan dikenakan policy atau kebijakan tersebut
   - Menentukan layanan-layanan yang di butuhkan oleh tiap tiap individu atau kelompok yang menggunakan jaringan

- Berdasarkan setiap layanan yang di gunakan oleh individu atau kelompok tersebut akan ditentukan bagaimana konfigurasi terbaik yang akan membuatnya semakin aman
- Menerapkankan semua policy atau kebijakan tersebut

3. Menyiapkan Software atau Hardware yang akan digunakan

   Baik sistem operasi yang mendukung atau software-software khusus pendukung firewall seperti ipchains, atau iptables pada linux, dsb. Serta konfigurasi hardware yang akan mendukung firewall tersebut.

4. Melakukan test konfigurasi

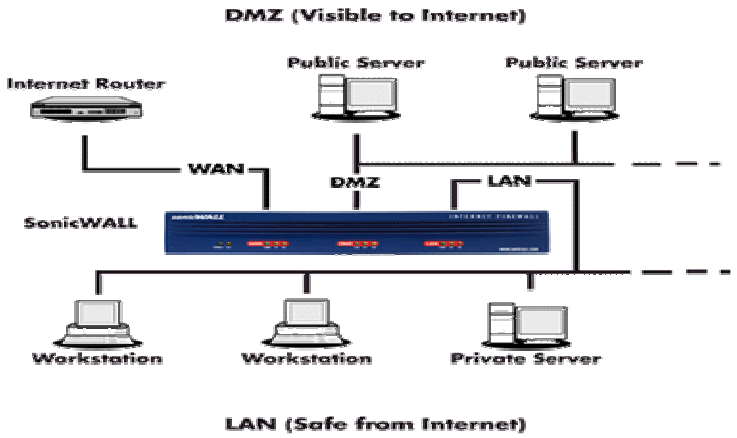
   Pengujian terhadap firewall yang telah selesai di bangun haruslah dilakukan, terutama untuk mengetahui hasil yang akan kita dapatkan, caranya dapat menggunakan tool tool yang biasa dilakukan untuk mengaudit seperti nmap.

- ***Bastion Host*** *adalah sistem/bagian yang dianggap tempat terkuat dalam sistem keamanan jaringan oleh administrator.atau dapat di sebuta bagian terdepan yang dianggap paling kuat dalam menahan serangan, sehingga menjadi bagian terpenting dalam pengamanan jaringan, biasanya merupakan komponen firewall atau bagian terluar sistem publik. Umumnya Bastion host akan menggunakan Sistem operasi yang dapat menangani semua kebutuhan (misal , Unix, linux, NT)*

2.2.3. Pengertian Demilitary Zone (DMZ)

DMZ adalah suatu “sacrificial lamb” bagi hackers yang digunakan untuk melindungi sistem internal yang berhubungan dengan serangan hack (hack attack). DMZ bekerja pada seluruh dasar pelayanan jaringan yang membutuhkan akses terhadap jaringan “dunia luar” ke bagian jaringan yang

lainnya. Dengan begitu, seluruh “open port” yang berhubungan dengan dunia luar akan berada pada jaringan, sehingga jika seorang hacker melakukan serangan dan melakukan crack pada server yang menggunakan sistem DMZ, hacker tersebut hanya akan dapat mengakses hostnya saja, tidak pada jaringan internal.



Gambar 2.9 : DMZ

Secara umum DMZ dibangun berdasarkan tiga buah konsep, yaitu : NAT (Network Address Translation), PAT (Port Addressable Translation), dan Access List. NAT berfungsi untuk menunjukkan kembali paket-paket yang datang dari “real address” ke alamat internal. Misal : jika kita memiliki “real address” 203.8.90.100, kita dapat membentuk suatu NAT langsung secara otomatis pada data-data yang datang ke 192.168.100.1 (sebuah alamat jaringan internal). Kemudian PAT berfungsi untuk menunjukan data yang datang pada particular port, atau range sebuah port dan protocol (TCP/UDP atau lainnya) dan alamat IP ke sebuah particular port atau range sebuah port ke sebuah alamat internal IP. Sedangkan access list berfungsi untuk mengontrol secara tepat apa yang datang dan keluar dari jaringan dalam suatu pertanyaan. Misal :

kita dapat menolak atau memperbolehkan semua ICMP yang datang ke seluruh alamat IP kecuali untuk sebuah ICMP yang tidak diinginkan.