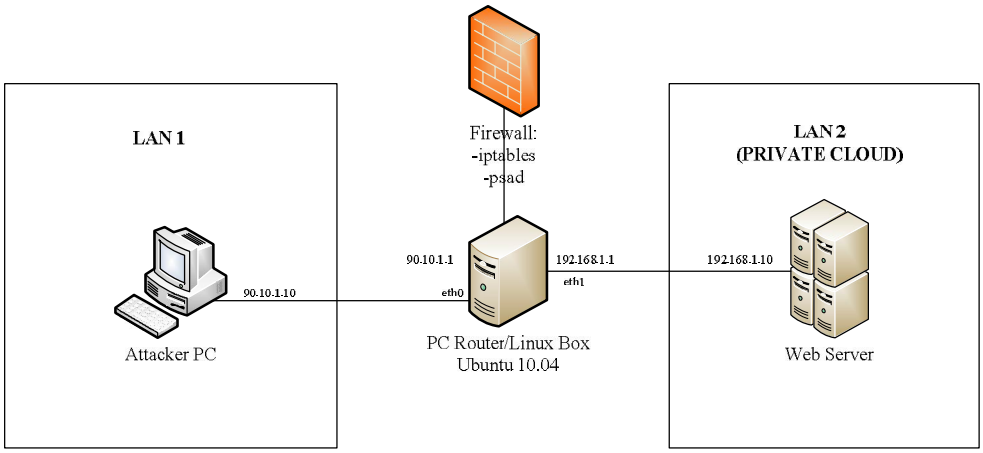
BAB III
PERANCANGAN SISTEM

3.1 Blok Sistem Secara Keseluruhan

Berikut merupakan gambar topologi perancangan sistem yang akan dibangun secara keseluruhan:



Gambar 3.1 Topologi Jaringan Yang Akan Dirancang

Komputer yang berfungsi sebagai PC Router menghubungkan jaringan LAN 1 dengan internet LAN 2. Pada PC Router terpasang 2 buah Network Interface Card (NIC). Masing-masing NIC terhubung kepada jaringan yang berbeda. Kedua NIC dikenal dengan eth0 dengan alamat IP 90.10.1.1 dan eth1 dengan alamat 192.168.1.1. Eth0 terhubung kepada sebuah komputer (dalam hal ini Attacker PC) yang berada pada LAN 1, sedangkan eth1 terhubung dengan jaringan LAN 2, dimana LAN 2 merupakan jaringan Private Cloud yang terdapat sebuah PC yang berfungsi sebagai Web Server. IP eth1 dan eth0 merupakan gateway (gerbang utama) paket untuk masuk atau keluar LAN 2.

`

3.2 Perancangan Sistem

Pada sistem yang akan dirancang terdapat 2 bagian penting, yaitu:

1. Perancangan Perangkat Keras
2. Perancangan Perangkat Lunak

3.2.1 Perancangan Perangkat Keras

Untuk perancangan perangkat keras, terdapat spesifikasi-spesifikasi perangkat keras yang digunakan terkait penelitian yang dilakukan dan digunakan, yaitu:

3.2.1.1 Spesifikasi PC Router

Berikut merupakan spesifikasi minimum perangkat keras untuk digunakan sebagai PC Router:

1. Prosesor Pentium 3
2. Memori 512 MB
3. Harddisk 20GB
4. Minimal NIC 2 buah

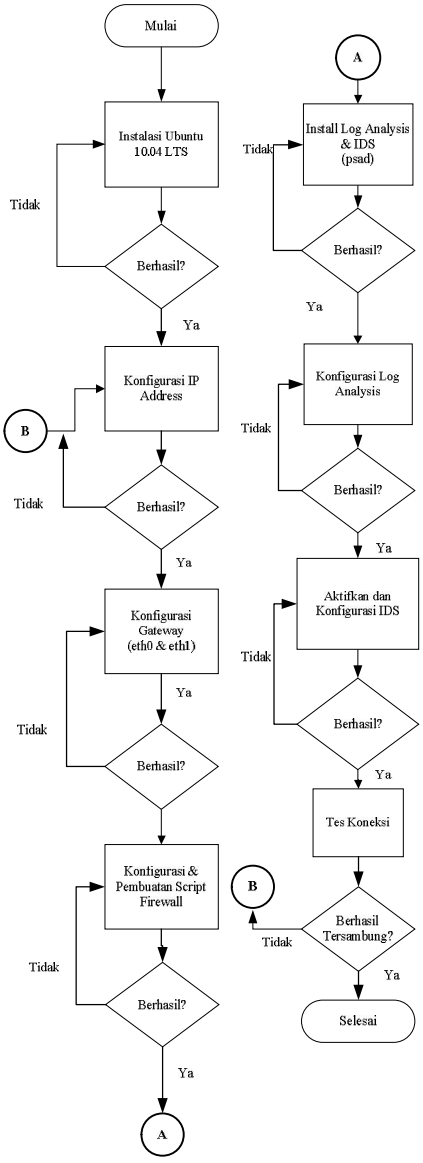
Sedangkan, berikut merupakan spesifikasi perangkat keras yang digunakan sebagai PC Router adalah:

1. Prosesor Intel Pentium Dual Core G 620 2,6 GHz
2. Memori 3 GB
3. Harddisk 80 GB
4. NIC 2 buah

Berdasarkan diagram alir pada gambar 3.2 dibawah, dapat dijelaskan bahwa hal pertama yang dilakukan adalah melakukan instalasi sistem operasi untuk digunakan sebagai PC Router. Sistem operasi yang digunakan adalah Linux Ubuntu 10.04 LTS. Setelah berhasil melakukan instalasi maka dilanjutkan melakukan konfigurasi IP Address. Pada PC Router ini menggunakan dua buah NIC. Selanjutnya adalah melakukan konfigurasi gateway sebagai gerbang masuk dan keluar LAN 1 dan jaringan LAN 2. Setelah melakukan konfigurasi gateway, maka selanjutnya adalah konfigurasi & pembuatan script rules dan policy firewall (Iptables) sebagai dasar perlakuan terhadap paket yang masuk/melewati untuk mengamankan jaringan private cloud dari luar. Kemudian setelah

`

mengkonfigurasi firewall maka tahap selanjutnya adalah melakukan instalasi dan konfigurasi Log Analysis dan IDS (psad) yang digunakan untuk menganalisis terhadap paket yang di log oleh firewall, kemudian setelah selesai maka dilanjutkan dengan mengaktifkan serta mengkonfigurasi IDS untuk melakukan blok alamat IP secara otomatis. Setelah semua konfigurasi selesai lakukan pengecekan koneksi apakah semua komponen yang akan diterapkan pada PC Router sudah berjalan sebagaimana mestinya atau tidak.



Gambar 3.2 Diagram alir Perancangan PC Router

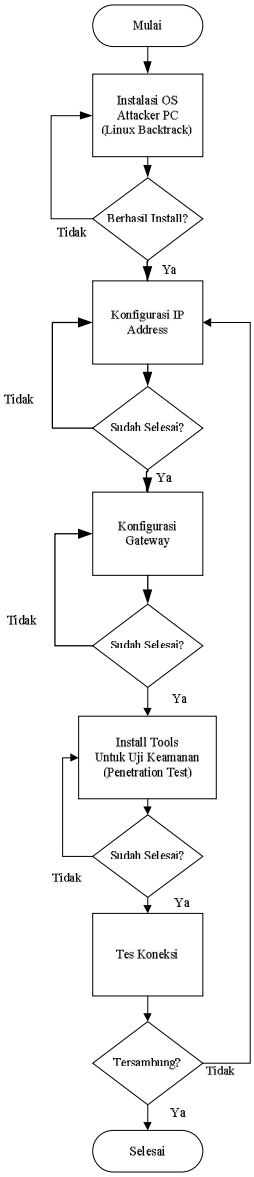
`

3.2.1.2 Spesifikasi Komputer Attacker PC

Berikut merupakan spesifikasi minimal perangkat keras/perangkat lunak yang dibutuhkan dari komputer yang akan digunakan sebagai Attacker PC:

1. OS Linux Backtrack 5 R3
2. Prosesor Pentium 4
3. Memori 512 MB
4. NIC 1 buah

Berikut merupakan diagram alir untuk perancangan komputer Attacker PC.



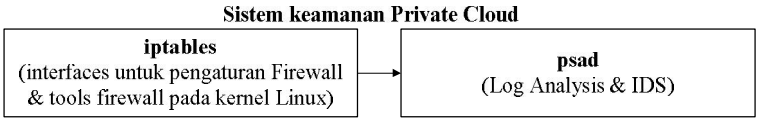
Gambar 3.3 Diagram Alir Perancangan Attacker PC

`

Attacker PC yang ditempatkan pada LAN 1, bertugas untuk melakukan serangkaian uji keamanan seperti port scan/port sweep dan DOS Attack tipe ICMP Flooding untuk menguji serta membuktikan apakan sistem keamanan firewall dan IDS pada PC Router dapat membuat Web Server Private Cloud lebih aman dan robust terhadap serangan dari luar.

3.2.2 Perancangan Perangkat Lunak

Selain dilakukan perancangan perangkat keras, dalam penelitian ini dilakukan juga perancangan perangkat lunak karena sistem keamanan yang dirancang berbasis perangkat lunak.



Gambar 3.4 Diagram Blok Penyusun Sistem Keamanan

Gambar 3.4 merupakan diagram blok untuk penyusun sistem keamanan. Dalam pengaturan firewall secara default pada setiap sistem operasi linux (distro manapun) menggunakan iptables. iptables digunakan untuk mengoperasikan serta mengatur firewall yang dimiliki linux yang sudah termasuk pada kernelnya yaitu netfilters. Sehingga dengan demikian dalam perancangan sistem keamanan firewall yang digunakan dalam penelitian ini adalah menggunakan software yang sudah ada pada linux itu sendiri yaitu netfilters dan digunakan antarmuka untuk pengkonfigurasiannya yaitu iptables. Apabila ada paket yang berbahaya/mencurigakan, maka iptables akan melakukan log pada paket tersebut dan kemudian di-drop. Agar log dari iptables dapat dianalisis lebih lanjut dan mudah dimengerti, maka digunakan tools tambahan sebagai Log Analysis Psad yaitu psad (port scan attack detector). Tetapi selain dapat digunakan sebagai log analysis, Psad memiliki fitur memblok suatu alamat IP secara otomatis apabila melebihi suatu batas toleransi yang ditentukan, yang dinamakan IDS (Intrusion Detection System).

Pada gambar 3.5 dibawah yang merupakan diagram alir untuk proses packet filtering dalam sistem keamanan firewall terdapat kata Rules, dan Rules sendiri merupakan suatu aturan yang dimana telah ditetapkan sebelumnya oleh

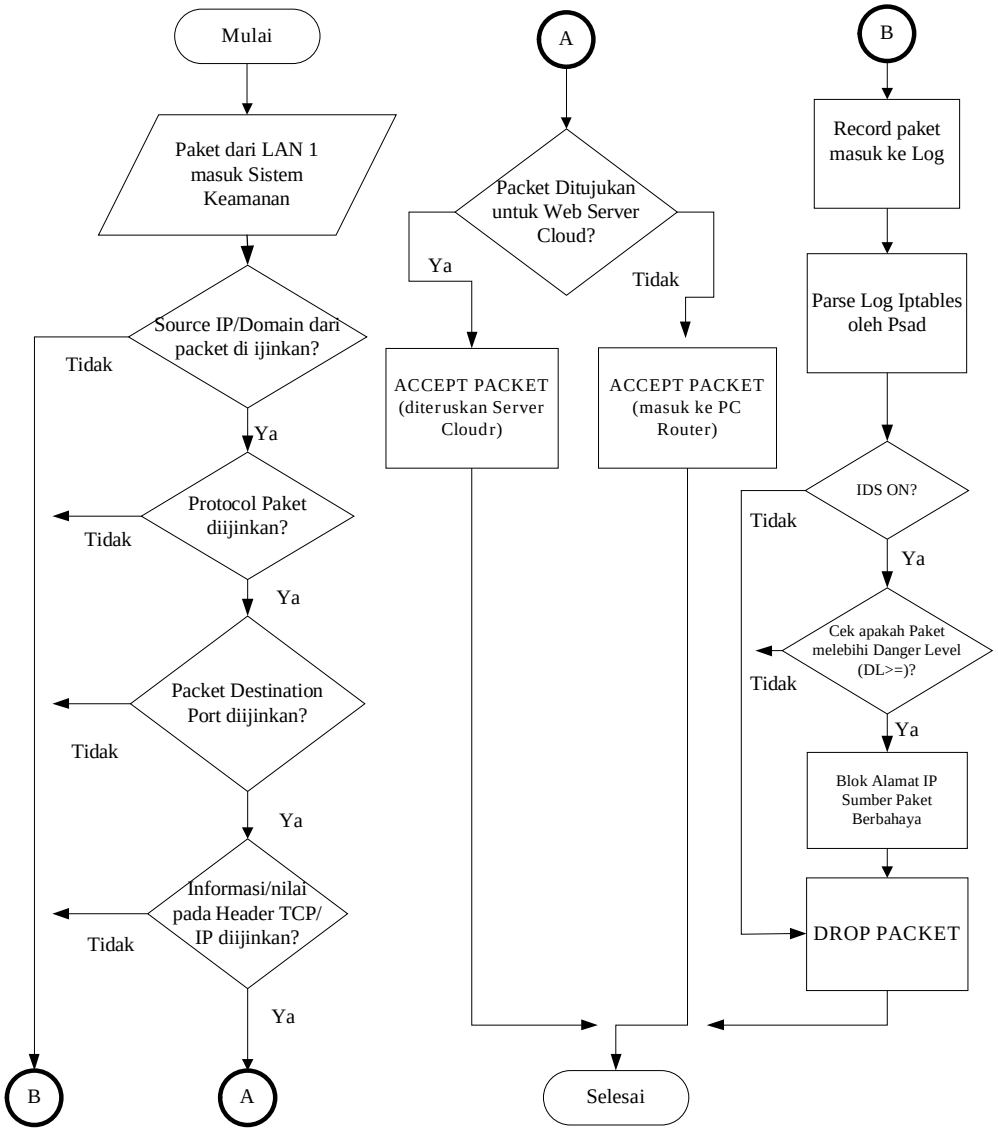
`

admin dalam pembangunan suatu sistem keamanan firewall yang dimana paket yang datang akan dibandingkan dengan rules tersebut apakah cocok, tidak cocok, dan apabila cocok dilakukan filtering atau tidak. Tetapi apabila paket yang datang tidak cocok dengan semua rules yang diterapkan, maka nasib paket tersebut akan ditetapkan sesuai dengan Policy pada sistem keamanan itu. Apakah paket itu Accept atau Drop.

Berikut merupakan Policy dan Rules yang akan diterapkan pada perancangan sistem keamanan firewall yang akan dilakukan:

1. Policy Drop All Packet (Positive List).
2. Pada PC Router akan digunakan dua buah NIC yang memiliki alamat masing-masing sebagaimana berikut:
   a. Eth0: 90.10.1.1 (terhubung ke LAN 1)
   b. Eth1: 192.168.1.1 (terhubung ke LAN 2)
3. Alamat Web Server adalah 192.168.1.10 .
4. Web Server diizinkan melakukan remote SSH ke PC Router.
5. Port yang dibuka pada PC Router adalah port tcp 80 (web/http), tcp 443 (https), tcp/udp 53 (DNS), tcp 22 (ssh).
6. Port yang dibuka pada PC Router dan diteruskan ke Web Server Private Cloud adalah traffic paket internet yang datang dari eth0 pada PC Router dan masuk ke port 80 dan 443 & 53 kemudian baru diteruskan kepada Web Server yang bersangkutan.
7. Web Server pada jaringan Private Cloud diijinkan melakukan koneksi TCP untuk port 80, 443, dan 53 hanya ketika ada permintaan (Request) dari luar (LAN 1) atau dengan kata lain, hanya boleh membalas tetapi tidak boleh melakukan koneksi sendiri.
8. Paket yang datang dari eth0 (LAN 1) yang memiliki alamat IP sumber (atau network) sama dengan LAN 2 (Private Cloud) di DROP.
9. Paket yang diijinkan masuk hanya paket yang termasuk kepada koneksinya yang sebelumnya telah dibangun dan masih berkaitan dengan koneksinya tersebut.
10. Selain paket yang diizinkan, maka paket yang lain akan di DROP oleh Firewall.

`



Gambar 3.5 Diagram Alir Packet Filtering & Sistem Keamanan

Untuk perancangan perangkat lunak, berikut akan dijelaskan perangkat lunak apa saja yang akan digunakan dalam penelitian ini:

3.2.2.1 Linux Ubuntu 10.04 LTS

Pada PC Router, sistem operasi yang akan digunakan adalah Linux Ubuntu 10.04 LTS yang dimana merupakan sistem operasi yang berbasis opensource dan untuk lebih lengkapnya dalam penginstalasian akan dijelaskan pada bagian lampiran.

`

3.2.2.2 Iptables/Netfilters

Untuk tools firewall yang akan digunakan dalam sistem keamanan nanti akan digunakan tools yang sudah ada pada sistem operasi yang digunakan atau pre-installed, yaitu menggunakan iptables/netfilters.

Berikut merupakan sintaks yang digunakan dalam pengkonfigurasian iptables:

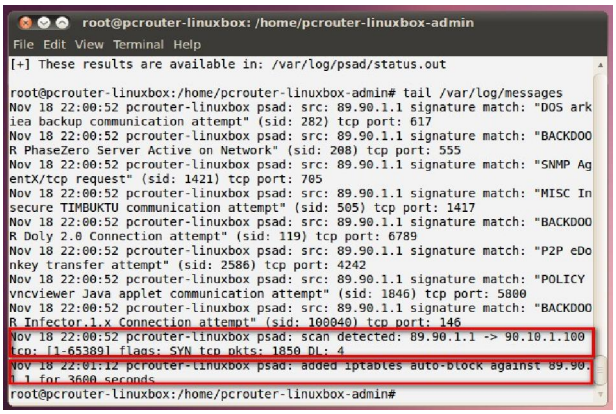
```
iptables [-t table] command [match] [target/jump]
```

Dari sintaks diatas maka berikut merupakan contoh sintaks untuk memblok semua protocol TCP yang datang untuk masuk ke port 80 (menutup layanan http):

```
iptables –A INPUT –p TCP --dport 80 –j DROP
```

3.2.2.3 Psad (Port Attack Scanner Detector)

Untuk melakukan log analysis dari file data log iptables untuk mendapatkan hasil log yang lebih dimengerti digunakanlah psad. Selain digunakan sebagai log analysis psad juga dapat digunakan sebagai pertahanan dari serangan layer transport dengan memanfaatkan fitur yang dimiliki iptables (--log-tcp-options) dengan melakukan log dan mengirim alert pada admin (IDS) serta bila diperlukan mempunyai fitur auto-block terhadap suatu IP karena telah melakukan serangan/reconnaissance terhadap sistem keamanan. Berikut merupakan contoh hasil laporan/status serta psad melakukan auto-block terhadap serangan yang dilakukan menggunakan nmap.



Gambar 3.6 Hasil Laporan dan Status Auto-blok IDS