BAB II

ANALISIS DAN PERANCANGAN

1. Analisis Kebutuhan

2.1.1 Pengertian *Hak akses*

Hak akses adalah bagian penting lainnya dari aspek multi user dari sebuah sistem berkas. Dengan hak akses anda dapat mengganti siapa saja yang dapat membaca, menulis, dan mengeksekusi berkas.

* + 1. Linux Ubuntu 9.04

Linus Torvalds adalah orang pertama yang membuat Linux yang berasal dari Filandia, tak heran jika linux di pakai menjadi nama operating system seperti nama penemunya Agustus 1991, Linus mengerjakan versi 0.01 dan pada tahun yang sama tepatnya pada tanggal 5 Oktober 1991, secara resmi meluncurkan versi 0.02.

Ubuntu berasal dari bahasa afrika yakni “Humanity to Others” yang berarti “Kemanusiaan untuk sesama” atas dasar itulah di luncurkan Linux Ubuntu yang dirilis pada tahun 2004. Sistem Operasi ini adalah merupakan turunan dari sistem Operasi Linux yang lain yakni Debian.di buat dengan tujuan selalu gratis tanpa adanya biaya lisensi, bersifat open source (kode terbuka), dan siap untuk di pergunakan dalam kondisi yang stabil.

Ubuntu di dukung oleh perusahaan bernama Canonical,Ltd yang memiliki tujuan untuk membantu perkembangan, distribusi, dan promosi dari produk - produk yang bersifat open source (kode terbuka).

Perusahaan ini bermarkas di Eropa dan di pimpin oleh seseorang bernama Mark Shuttleworth. Sejak pertama kali di luncurkan, Ubuntu mendapat perhatian yang sangat besar dari pengguna Linux yang lain. Hal ini di sebabkan karena kestabilan yang di miliki oleh Ubuntu itu sendiri. Selain itu kenyamanan dan kemudahan yang di miliki Ubuntu menjadi daya tarik yang besar bagi pengguna Linux di seluruh belahan dunia.

* + 1. Proxy Server

Adalah teknik yang standart untuk akses internet secara bersama-sama oleh beberapa komputer sekaligus dalam sebuah Local Area Network (LAN) melalui sebuah modem atau sebuah saluran komunikasi.

Istilah Proxy sendiri banyak dikenal atau digunakan terutama di dunia atau kalangan diplomatik.Secara sederhana Proxy adalah seseorang atau lembaga yag bertindak sebagai perantara atau atas nama dari orang lain atau lembaga

Proxy Server adalah sebuah komputer server atau program yang dapat bertindak sebagai komputer lainnya untuk melakukan request terhadap content dari internet atau intranet.

Proxy server bertindak sebagai gateway terhadap dunia internet untuk setiap komputer klien. Proxy server tidak terlihat oleh komputer klien seorang pengguna yang berinteraksi dengan internet melalui sebuah proxy server tidak akan mengetahui bahwa sebuah proxy server sedang menangani request yang dilakukannya web server yang menerima request dari proxy server akan menginterpretasikan request - request tersebut seolah - olah request itu datang secara langsung ke komputer client bukan dari proxy server.

Proxy server juga dapat di gunakan untuk mengamankan jaringan pribadi yang di hubungkan ke sebuah jaringan publik (seperti hanya Internet). Proxy server memiliki lebih banyak lebih banyak fungsi daripada router yang memiliki fitur paket filtering karena memang proxy server beroperasi pada level yang lebih tinggi dan memiliki kontrol yang lebih menyeluruh terhadap akses jaringan Proxy server yang berfungsi

Sebagai sebuah “agen keamanan” untuk sebuah jaringan pribadi,umumnya dikenal sebagai firewall.

* Internet Sharing Server (ISS) – biasanya berupa hardware berdiri sendiri lengkap dengan modem,hub dan software proxy di dalamnya.
* Network Address Translation (NAT) – istilah lain yang digunakan untuk software proxy server.
* IP masquerade – teknik yang di gunakan di software NAT / Proxy server untuk melakukan proses proxy.
  + 1. Squid

Squid adalah software proxy server yang bersifat open source yang sangat terkenal, cara kerja squid dapat di analogikan seperti browser yang menyimpan data suatu site di hardisk sehingga untuk menampilkan site yang sama tinggal mengambil data cachenya Squid berlisensi GPL (GNU public License). Squid dalam sejarah pmbuatannya merupakan produk turunan dari harvest Cache (dibuat oleh Harvest project, <http://harvest.cs.colorado.edu/>) dan nama squid dipilih oleh pembuatannya karena nama bagus lainnya sudah diambil orang lain (dari FAQ 1 squid) masih dari sumber yang sama squid dikatakan sebagai server proxy cache yang mempunyai performasi tinggi dan mendukung operasional [FTP.Ghopher](ftp://FTP.Ghopher) dan HTTP dalam memenuhi permintaan client, squid menangani dalam satu proses I/O (input/Output) dan tidak bersifat blocking. Squid dibuat oleh sebuah komunitas internet dan di pimpin oleh Duanne Wessel dari national laboratory For Applied Network Reseach yang di biayai oleh National Science Foundation.List dari kontributor dapat dilihat di <http://www.squid-cache.org/CONTRIBUTORS>

* + 1. Setting Policy

Dalam hal ini penyetinggan policy dilakukan agar keamanan jaringan dapat terkendali, nantinya policy ini akan ditentukan oleh server yang akan diberlakukan pada clien sehingga tidak semua user dapat mengakses data yang telah setting policy.

Serverpun akan memberikan password sehingga hanya server itu sendiri yang akan mengaksesnya. Pengaturan default user, group maupun komputer yang tergabung dalam domain yang bersangkutan. Banyak yang dapat diatur dalam group policy object (GPO) Default Domain Policy ini, hanya beberapa yang nanatinya akan diset ulang pengaturannya.

* + 1. Iptables

Untuk bisa mengetahui jumlah keluar/masuknya paket data untuk suatu komputer kita harus menghitungnya secara terpisah yaitu untuk yang masuk dan untuk yang keluar. Bila kita akan mengamati sepuluh komputer, maka setidaknya harus ada 20 rule iptables. Chain yang digunakan untuk mengamati adalah chain FORWARD.

Untuk memudahkan pengamatan & persaingan nilai hitungan iptables kita dapat menambahkan masing-masing 2 chain kosong yang menjadi target rule sehingga memudahkan kita dalam menjalankan grep, misal dengan menggunakan nama komputer yang kita beri tambahan –in dan –out

INPUT

Mengatur paket data yang memasuki firewall dari arah intranet maupun internet. Kita bisa meneglola komputer mana yang bisa mengakses firewall. Misal hanya komputer IP address 192.168.1.100 yang bisa SSH ke firewall dan yang lain tidak boleh.

OUTPUT

Mengatur paket data yang keluar dari firewall ke arah intranet maupun internet. Biasanya output tidak diset, karena bisa membatasi kemampuannya firewall itu sendiri.

FORWARD

Mengatur paket data yang melintasi firewall dari arah internet ke intranet maupun sebaiknya. Policy forward paling banyak dipakai saat ini untuk mengatur koneksi internet berdasarkan port, mac address dan alamat IP. Selain aturan (policy) firewall iptables juga mempunyai parameter yang disebut dengan TARGET, yaitu status yang menentukan koneksi iptables diizinkan lewat atau tidak TARGET ada tiga macam yaitu

* ACCEPT

Akses diterima dan diizinkan firewall

* REJECT

Akses ditolak,koneksi dari komputer client yang melewati firewall langsung terputus, biasanya terdapat “Connection Refused”. Target Reject tidak menghabiskan bandwidth internet akses langsung ditolak, hal ini berbeda dengan DROP.

* DROP

Akses diterima tetapi pakes data langsung dibuang oleh kernel, sehingga pengguna tidak mengetahui kalau koneksinya dibatasi oleh firewall, pengguna melihat seakan-akan server yang dihubungi mengalami permasalahn teknis. Pada koneksi internet yang sibuk dengan trafik tinggi Target Drop sebaiknya jaangan digunakan.

Pada iptables jika ingin memblokir suatu website maka megetikkan perintah:

Iptables –A INPUT –m string –algo kmp –string youtube –j REJECT

Perintah tersebut di gunakan untuk satu URL maka perintahnya kan semakin banyak menggunakan squid sedikit lebih sederhana ,hanya membuat ACL (Access Control List) yang berisi path URL yang di blok dan tinggal dibatalkan saja dengan menekan tombol deny.

Pertama kali d buat file yang berisi URL yang di blok.

Editor/etc/squid/urlblox.txt

Isi file tersebut dengan URL yang ingin diblok

youtube.com

facebook.com

Selanjutnya membaca ACL dan deny ACL tersebut di file squid.conf

Acl blokurl dstdomain /etc/squid/urlblok.txt

http\_access deny blokurl

* + 1. Router

*Router* adalah sebuah [alat jaringan komputer](http://id.wikipedia.org/w/index.php?title=Alat_jaringan_komputer&action=edit&redlink=1) yang mengirimkan [paket](http://id.wikipedia.org/wiki/Paket_jaringan) [data](http://id.wikipedia.org/wiki/Data) melalui sebuah [jaringan](http://id.wikipedia.org/wiki/Jaringan_komputer) atau [internet](http://id.wikipedia.org/wiki/Internet) menuju tujuannya melalui sebuah proses yang dikenal sebagai [*routing*](http://id.wikipedia.org/wiki/Routing)*. Router* berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya.

Router yang di gunakan untuk menghubungkan LAN ke sebuah koneksi leased line sering di sebut sebagai *accesss server*.Router umumnya memblokir lalu lintas data yang di pancarkan secara *broadcast* sehingga dapat mencegah adanya *broadcast strom* yang mampu memperlambat kinerja jaringan.

* + 1. Alat dan Bahan

Tabel 2.1 Alat dan Bahan

|  |  |  |  |
| --- | --- | --- | --- |
| **NO** | **Alat** | **Spesifikasi** | **Volume** |
| 1 | Proccessor | Pentium IV | 1 |
| 2 | RAM | 256 MB | 1 |
| 3 | Hardisk | 20 GB | 1 |
| 4 | CD Linux Ubuntu Server 9.04 |  | 1 |
| 5 | LandCard | Realtek RTL 8110 | 2 |
| 6 | Switch(DLink) | 8 port | 1 |
| 7 | Kabel UTP |  | Secukupnya |
| 8 | Konektor RJ45 |  | Secukupnya |
| 9 | Modem | Linksys AM300 | 1 |

2.1.9 Perancangan

2.

Hotspot

192.168.50.1.4/28

Server



IP Modem :

192.168.50.3/28



Eth0 : 192.168.50.2/28

Modem ADSL Speedy

Eth1: 192.168.50.1/28







192.168.50.5/28



192.168.50.11/28



192.168.50.7/28

192.168.50.8/28

192.168.50.10/28

192.168.50.6/28

192.168.50.9/28

Gambar 2.2 Diagram jaringan