PENERAPAN CAPTIVE PORTAL PADA WIFI HOTSPOT DALAM PENJUALAN VOUCHER INTERNET

TUGAS AKHIR

Oleh :

Maria Eva Manda Arindika **3310701116**

Disusun untuk memenuhi syarat kelulusan Program Diploma III

PROGRAM STUDI APLIKASI PERANGKAT LUNAK

JURUSAN TEKNIK INFORMATIKA

POLITEKNIK BATAM

BATAM

2010

LEMBAR PENGESAHAN

Batam, 1 maret 2010

Pembimbing,

Uuf Brajawidagda, MT

NIK. 100015

LEMBAR PERNYATAAN

Dengan ini, saya:

NIM : 3310701116

Nama : Maria Eva Manda Arindika

adalah mahasiswa Teknik Informatika Politeknik Batam yang menyatakan bahwa tugas akhir dengan judul:

Penerapan Captive Portal pada Wifi Hotspot dalam Penjualan Voucher Internet

disusun dengan:

1. tidak melakukan plagiat terhadap naskah karya orang lain
2. tidak melakukan pemalsuan data
3. tidak menggunakan karya orang lain tanpa menyebut sumber asli atau tanpa ijin pemilik

Jika kemudian terbukti terjadi pelanggaran terhadap pernyataan di atas, maka saya bersedia menerima sanksi apapun termasuk pencabutan gelar akademik.

Lembar pernyataan ini juga memberikan hak kepada Politeknik Batam untuk mempergunakan, mendistribusikan ataupun memproduksi ulang seluruh hasil Tugas Akhir ini.

Batam, 1 maret 2010

Maria Eva Manda Arindika
NIM. 3310701116

KATA PENGANTAR

Puji dan syukur kehadirat Tuhan Yang Maha Esa atas berkat dan karuniaNya, penulis dapat menyelesaikan Tugas Akhir sesuai dengan waktu yang telah ditentukan. Penelitian terhadap perbandingan software captive portal dibuat dengan tujuan untuk mengetahui kelebihan dan kelemahan antara software captive portal yang satu dengan yang lain, serta dapat menjadi acuan bagi pengelola wifi hotspot dalam melakukan pemilihan software captive portal yang tepat. Dalam kesempatan ini pula penulis mengucapkan terima kasih kepada:

1. Bapak Ir. Priyono Eko Sanyoto selaku direktur Politeknik Batam
2. Bapak Uuf Brajawidagda, MT selaku koordinator Tugas Akhir dan dosen pembimbing
3. Bapak Indratno selaku pemberi ide/konsep dalam pencarian judul Tugas Akhir
4. Dosen program studi Teknik Informatika atas bimbingannya
5. Teman-teman APL yang telah memberikan semangat dan pertolongan
6. Keluarga yang telah memberikan doa serta dukungan
7. Semua pihak yang telah memberikan doa dan dukungannya

Penulis menyadari bahwa masih banyak kekurangan dalam penyusunan laporan ini. Oleh karena itu penulis sangat mengharapkan bantuan dari beberapa pihak baik berupa kritik maupun saran guna untuk penyempurnaan selanjutnya. Akhir kata penulis mengucapkan terima kasih, semoga penulisan laporan ini dapat bermanfaat bagi pembaca yang ingin mengembangkan sebuah penelitian yang serupa.

Batam, maret 2010

Penulis

ABSTRAKSI

Penerapan Captive Portal pada Wifi Hotspot dalam Penjualan Voucher Internet

Captive Portal adalah sebuah perangkat lunak yang dapat digunakan untuk mengelola wifi hotspot. Software ini digunakan untuk memverifikasi pengguna sebelum mengizinkan mereka mengakses internet dari jaringan lokal. Karena ada banyak software captive portal yang tersedia, maka diperlukan suatu panduan yang dapat digunakan dalam memilih software captive portal. Tujuan dari dokumen ini adalah untuk memudahkan pengguna dalam memilih software captive portal yang tepat sesuai dengan kebutuhan pengguna. Software captive portal yang dibandingkan dalam dokumen ini yakni monowall, pfsense, dan easy hotspot.

Kata kunci: Captive portal, wifi hotspot.

ABSTRACT

Captive Portal Implementation on Wifi Hotspot for an Internet Voucher Sale

Captive Portal is a software that can be used to manage wifi hotspot. This software is to verify the user before allowing them to access the internet from a local network. Since there are many captive portal software available, a guidance to choose a captive portal software is needed. The aim of this document is to ease the user to choose the right captive portal software suitable for the user needs. The captive portal software which are compared in this document is monowall, pfsense, and easy hotspot.

Keyword: Captive portal, wifi hotspot.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1 PENDAHULUAN

1.1 Latar Belakang

Wifi hotspot merupakan area bagi pengguna untuk melakukan akses internet, proses pengelolaan wifi hotspot dapat dilakukan dengan memanfaatkan captive portal. Captive portal merupakan software yang dapat digunakan untuk memverifikasi pengguna, software ini dapat diterapkan pada jaringan yang terhubung dengan koneksi internet. Proses verifikasi ini dapat menentukan keabsahan pengguna sebelum melakukan pemanfaatan jaringan internet. Pilihan dalam pemanfaatan captive portal untuk memberikan proses verifikasi user cukup beragam. Untuk melakukan pemilihan captive portal yang tepat, dapat dilakukan melalui proses perbandingan antara berbagai captive portal yang ada berdasarkan kriteria yang dipergunakan. Berdasarkan proses perbandingan tersebut maka dapat diketahui kelebihan dan kelemahan dari masing-masing software, serta membantu dalam menentukan pilihan software yang tepat sebelum diterapkan pada jaringan yang terhubung dengan internet.

1.2 Rumusan Masalah

Banyaknya pilihan software captive portal yang dapat dipergunakan untuk mengelola wifi hotspot.

1.3 Batasan Masalah

1. Proses perbandingan hanya akan dilakukan pada beberapa software captive portal saja, tidak dilakukan pada semua software captive portal.
2. Software captive portal yang akan diuji untuk proses perbandingan adalah software captive portal open source, bukan komersial (berbayar).
3. Proses pengujian tidak dilakukan pada berbagai bentuk topologi jaringan komputer.
4. Proses pengujian dikhususkan pada kriteria pembanding dalam pemilihan sebuah captive portal.
5. Fitur-fitur yang terdapat dalam software captive portal tidak bisa diuji secara keseluruhan karena terbatasnya fasilitas yang diperlukan.

1.4 Tujuan Penelitian

Tujuan dan manfaatnya adalah:

- Untuk mengetahui kelebihan dan kelemahan antara software captive portal yang satu dengan yang lain.
- Dapat menjadi acuan bagi pihak yang membuka akses internet untuk umum, dalam pemilihan software captive portal yang tepat.

1.5 Sistematika Penulisan

Laporan ini terdiri dari Bab Pendahuluan, Landasan Teori, Pemilihan dan Perancangan Pengujian Captive Portal, Implementasi dan Pembahasan, Kesimpulan dan Saran serta Lampiran yang berhubungan dengan proses pengujian.

Bab 1 Pendahuluan berisi penjelasan mengenai latar belakang masalah dalam proses penelitian, perumusan masalah, batasan masalah dalam proses penelitian, tujuan penelitian, dan sistematika penulisan untuk memberikan gambaran isi laporan tugas akhir.

Bab 2 Landasan Teori berisi tentang studi literatur yang digunakan sebagai referensi dalam proses penelitian yakni definisi captive portal, definisi router, definisi open source, berbagai bentuk topologi jaringan.

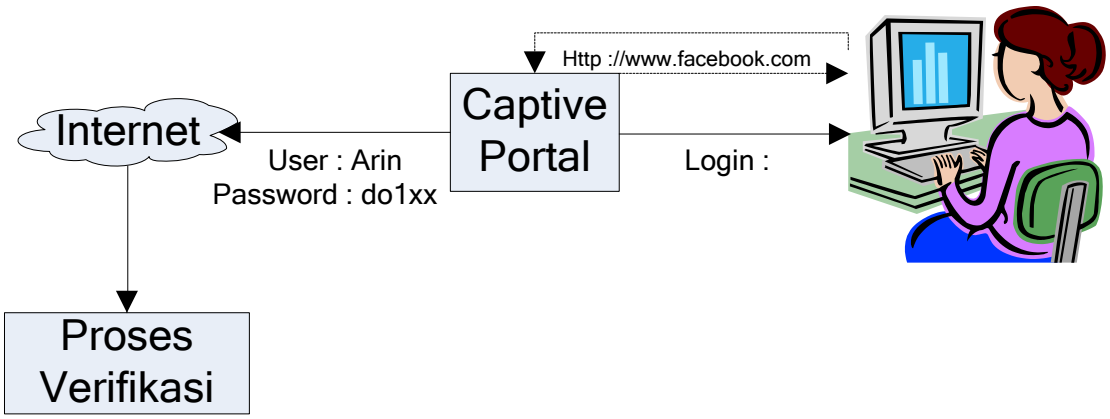
Bab 3 Pemilihan dan Perancangan Pengujian Captive Portal berisi tentang urutan proses/langkah dalam melakukan pemilihan software captive portal, jenis dan software captive portal, software-software yang digunakan dalam proses perbandingan, serta perancangan pengujian software captive portal yang meliputi skema jaringan, lingkungan pengujian dan kriteria evaluasi.

Bab 4 Implementasi dan pembahasan berisi tentang proses implementasi PC router, software-software captive portal, evaluasi software captive portal berdasarkan kriteria yang dipergunakan, perbandingan antara software-software captive portal.

Bab 5 Kesimpulan dan Saran berisi tentang penyimpulan hasil dari proses implementasi dan pembahasan pada bab sebelumnya, serta saran sebagai bahan pertimbangan untuk pengembangan penelitian selanjutnya.

BAB 2 LANDASAN TEORI

2.1 Definisi Captive Portal



Gambar 2.1 Definisi Captive Portal

Captive portal biasanya di tempatkan pada satu server yang bekerja sebagai router atau gateway, ketika user yang berada pada LAN atau wireless LAN hendak melakukan akses internet, server gateway akan memproteksi atau tidak mengizinkan adanya trafik sehingga akan mengalihkan paket data ke captive portal. Bentuk captive portal berupa web based authentication yang menyediakan halaman web berisi form untuk login. Setelah user memasukkan data verifikasi (biasanya berupa username atau password) maka user dapat melakukan akses pada jaringan. (Rob Flickenger, et. al., 2007)

Captive portal merupakan satu set perangkat lunak yang saling bekerja sama untuk melakukan tugasnya, beberapa perangkat lunak tersebut diantaranya:

1. Remote Access Dial Up service (RADIUS) Server, berfungsi untuk menangani sambungan dari jarak jauh. Dalam server ini juga diatur manajemen akses yang diberikan kepada pengguna seperti misalnya perhitungan penggunaan baik berdasarkan waktu ataupun data yang di download.

2. Dinamic Host Control Protocol (DHCP) Server, berfungsi untuk mengatur penggunaan IP address untuk user yang mengakses jaringan wireless.
3. Domain Name Sistem (DNS), merupakan sistem yang menyimpan informasi mengenai nama domain maupun nama host yang tersebar didalam jaringan komputer.
4. DNS Redirector, merupakan pengalih permintaan HTTP dari klien untuk di alihkan ke halaman atau alamat tertentu, misalnya halaman login, halaman persetujuan atau halaman peringatan.

Berikut merupakan cara kerja captive portal:

1. User dengan wireless client diizinkan untuk terhubung pada jaringan untuk mendapatkan IP address (DHCP)
2. Block semua trafik kecuali yang menuju ke captive portal (registrasi/verifikasi berbasis web) yang terletak pada jaringan kabel/nirkabel.
3. Redirect atau belokkan semua trafik web ke captive portal
4. Setelah user melakukan registrasi atau login, izinkan akses ke jaringan internet.

2.2 Definisi Router

Router adalah komputer general purpose (untuk tujuan yang lebih luas) dengan dua atau lebih interface jaringan (NIC Card) di dalamnya yang berfungsi menghubungkan 2 jaringan atau lebih, sehingga dapat meneruskan paket dari satu jaringan ke jaringan yang lain. Untuk jaringan kecil, interface-nya adalah NIC Card, sehingga router mempunyai 2 NIC atau lebih yang bisa menghubungkan dengan jaringan lain. Untuk LAN kecil yang terhubung internet, salah satu interface adalah NIC card, dan interface yang lain adalah sembarang hardware jaringan misal modem untuk leased line atau ISDN atau koneksi internet ADSL yang digunakan. (Rob Flickenger, et. al., 2007)

Tipe router:

1. Komputer yang di fungsikan sebagai router (PC Router).
2. Peralatan khusus yang dirancang sebagai router.

2.3 Definisi Open Source

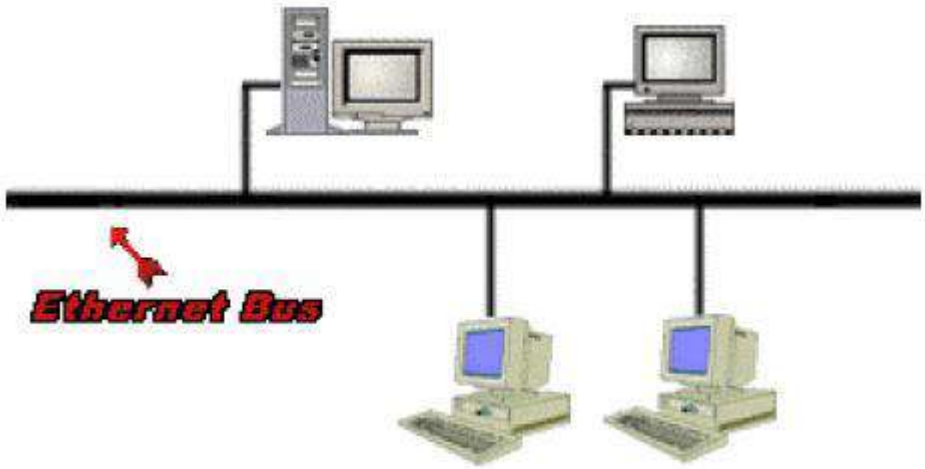
Open source software adalah istilah yang digunakan untuk software yang membuka/membebaskan source codenya untuk dilihat oleh orang lain, dan membiarkan orang lain mengetahui cara kerja serta memperbaiki kelemahan-kelemahan yang ada pada software tersebut. Syarat-syarat distribusi open source software harus memenuhi kriteria-kriteria berikut(The Opensource definition):

1. Distribusi ulang gratis.
2. Kode sumber harus disertakan.
3. Mengizinkan modifikasi dan penerusan hasil kerja oleh orang lain, serta izin untuk pendistribusian di bawah lisensi yang sama dengan software aslinya.
4. Lisensi dapat melarang kode sumber untuk didistribusikan ulang dalam bentuk termodifikasi, hanya jika lisensi mengizinkan distribusi file-file tambahan beserta kode sumber untuk tujuan memodifikasi program pada masa pembangunan.
5. Tidak ada diskriminasi terhadap pribadi atau golongan.
6. Tidak ada diskriminasi terhadap bidang atau usaha tertentu.
7. Hak-hak yang dimiliki oleh program harus dapat diaplikasikan oleh semua orang yang menerima distribusi program tersebut, tanpa perlu penambahan lisensi oleh pihak-pihak yang bersangkutan.
8. Lisensi tidak spesifik untuk satu produk(hak-hak yang dimiliki program bukan karena program tersebut menjadi bagian distribusi software tertentu).
9. Lisensi tidak boleh melakukan pembatasan terhadap software lain yang didistribusikan bersama dengan software yang diberi lisensi.
10. Lisensi harus netral terhadap teknologi(tidak ada syarat lisensi yang merupakan predikat dari suatu teknologi atau gaya antarmuka tertentu).

2.4 Topologi Jaringan

Topologi adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Cara yang saat ini banyak digunakan adalah bus, token-ring, star dan peer-to-peer network. Masing-masing topologi ini mempunyai ciri khas, dengan kelebihan dan kekurangannya sendiri. Berdasarkan topologi jaringan, jaringan komputer dapat dibedakan atas topologi Bus, topologi Bintang, topologi Cincin, topologi Mesh, topologi Pohon (Tree) dan Topologi Hybrid (Campuran). (I Putu Suardika, et. al., 2007)

2.4.1 Topologi Bus



Gambar 2.4.1 Topologi Bus

Topologi bus merupakan topologi yang banyak dipergunakan pada masa penggunaan kabel coaxial menjamur. Dengan menggunakan T-Connector (dengan terminator 50 ohm pada ujung network), komputer atau perangkat jaringan lainnya bisa dengan mudah dihubungkan satu sama lain. Kesulitan utama dari penggunaan kabel coaxial adalah sulit untuk mengukur apakah kabel coaxial yang dipergunakan benar-benar matching atau tidak. Karena, kalau tidak sungguh-sungguh diukur secara benar akan merusak NIC (Network Interface Card) yang dipergunakan dan kinerja jaringan menjadi terhambat, sehingga tidak mencapai kemampuan maksimalnya. Topologi ini juga sering digunakan pada jaringan dengan basis fiber optic (yang kemudian diganbungkan dengan topologi star untuk menghubungkan dengan client atau node).

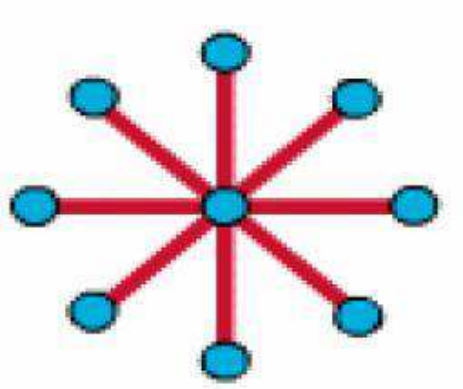
Keuntungan:

- Hemat kabel
- Layout kabel lebih sederhana
- Mudah dikembangkan

Kerugian:

- Deteksi dan isolasi kerusakan sangat kecil
- Kepadatan lalu-lintas
- Bila salah satu client rusak, maka jaringan tidak bisa berfungsi
- Diperlukan repeater untuk jarak jauh

2.4.2 Topologi Star



Gambar 2.4.2 Topologi Star

Pada topologi ini kita sudah menggunakan bantuan alat lain untuk mengkoneksikan jaringan komputer. Contoh alat yang di pakai disini adalah hub, switch, dan lain-lain. HUB atau Switch digunakan untuk menghubungkan setiap node dalam jaringan LAN. Peralatan ini sering digunakan pada topologi star dan extended star. Perbedaan antara HUB dan Switch adalah kecepatan transfer datanya yaitu 10:100 Mbps. Topologi jaringan ini banyak digunakan di berbagai tempat, karena kemudahan untuk menambah, mengurangi atau mendeteksi kerusakan jaringan yang ada. Selain itu, permasalahan panjang kabel yang harus sesuai (matching) juga tidak menjadi suatu yang penting lagi. Dengan berbekal crimtool, kabel UTP

(biasanya CAT5) dan connector, seseorang dengan mudah membuat sebuah sistem jaringan. Tentu ada beberapa kerugian karena panjang kabel (loss effect) maupun karena hukum konduksi, namun hampir bisa dikatakan semua itu bisa diabaikan. Prinsip topologi bintang adalah merupakan kontrol terpusat, semua link harus melewati pusat yang menyalurkan data tersebut kesemua simpul atau client yang dipilihnya. Simpul pusat dinamakan stasium primer atau server dan lainnya dinamakan stasiun sekunder atau client server. Setelah hubungan jaringan dimulai oleh server maka setiap client server sewaktu-waktu dapat menggunakan hubungan jaringan tersebut tanpa menunggu perintah dari server. Terdapat keuntungan dan kerugian dari tipe ini yaitu:

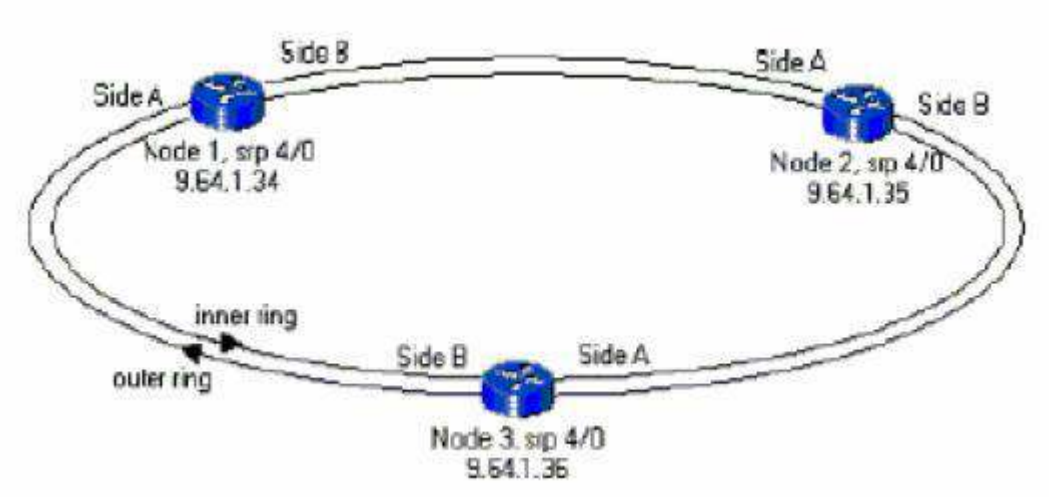
Keuntungan:

- Paling fleksibel
- Pemasangan/perubahan stasiun sangat mudah dan tidak menggangu bagian jaringan lain.
- Kontrol terpuat
- Kemudahan deteksi dan isolasi kesalahan/kerusakan
- Kemudahan pengelolaan jaringan

Kerugian:

- Boros kabel
- Perlu penanganan khusus
- Kontrol terpusat jadi elemen kritis

2.4.3 Topologi Ring



Gambar 2.4.3 Topologi Ring

Topologi cincin atau yang sering disebut dengan ring topologi adalah topologi jaringan dimana setiap komputer yang terhubung membuat lingkaran. Dengan artian setiap komputer yang terhubung kedalam satu jaringan saling terkoneksi ke dua komputer lainnya sehingga membentuk satu jaringan yang sama dengan bentuk cincin. Adapun kelebihan dari topologi ini adalah kabel yang digunakan bisa lebih dihemat. Tetapi kekurangan dari topologi ini adalah pengembangan jaringan akan menjadi susah karena setiap komputer akan saling terhubung.

Untuk membentuk jaringan cincin, setiap sentral harus dihubungkan seri satu dengan yang lain dan hubungan ini akan membentuk loop tertutup. Dalam sistem ini setiap sentral harus dirancang agar dapat berinteraksi dengan sentral yang berdekatan maupun berjauhan. Dengan demikian kemampuan melakukan switching ke berbagai arah sentral. Keuntungan dari topologi jaringan ini antara lain tingkat kerumitan jaringan rendah (sederhana), juga bila ada gangguan atau kerusakan pada suatu sentral maka aliran trafik dapat dilewatkan pada arah lain dalam sistem. Topologi yang paling banyak digunakan dalam jaringan komputer adalah jaringan bertipe bus dan pohon (tree), hal ini karena alasan kerumitan, kemudahan instalasi dan pemeliharaan serta harga yang harus dibayar. Tapi hanya jaringan bertipe pohon (tree) saja yang diakui kehandalannya karena putusnya salah satu kabel pada client, tidak akan mempengaruhi hubungan client yang lain.

Topologi ini merupakan kontrol terpusat, semua link harus melewati pusat yang menyalurkan data tersebut kesemua simpul atau client yang dipilihnya. Simpul pusat dinamakan stasiun primer atau server dan lainnya dinamakan stasiun sekunder atau client server. Setelah hubungan jaringan dimulai oleh server maka setiap client server sewaktu-waktu dapat menggunakan hubungan jaringan tersebut tanpa menunggu perintah dari server. Topologi ini memanfaatkan kurva tertutup, artinya informasi dan data serta traffic disalurkan sedemikian rupa sehingga masing-masing node. Umumnya fasilitas ini memanfaatkan fiber optic sebagai sarananya (walaupun ada juga yang menggunakan twisted pair).

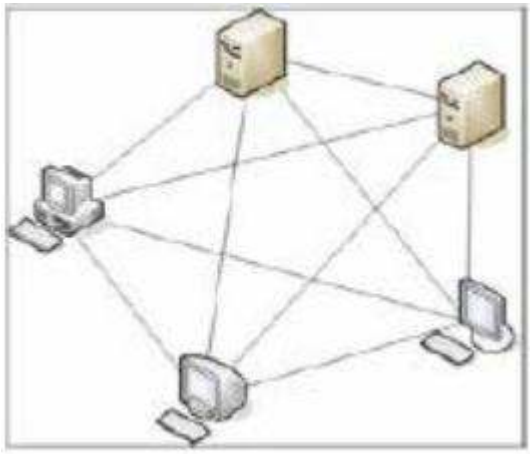
Keuntungan:

- Hemat kabel

Kerugian:

- Peka kesalahan
- Pengembangan jaringan lebih kaku

2.4.4 Topologi Mesh



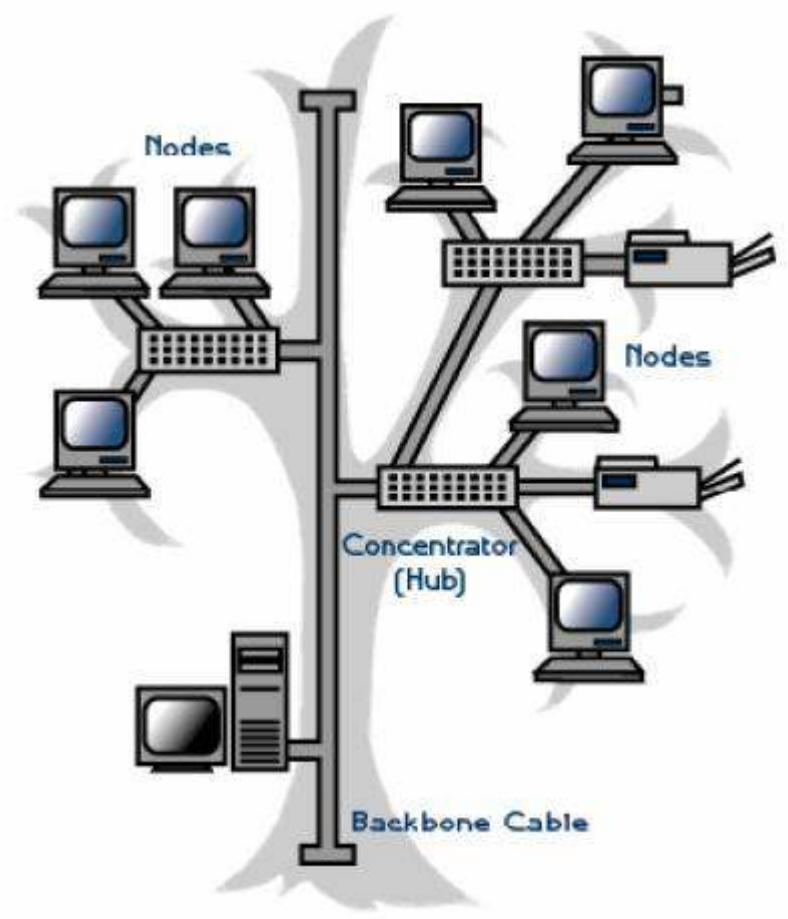
Gambar 2.4.4 Topologi Mesh

Topologi jaringan ini menerapkan hubungan antar sentral secara penuh. Jumlah saluran harus disediakan untuk membentuk jaringan Mesh adalah jumlah sentral dikurangi 1 (n-1, n = jumlah sentral). Tingkat kerumitan jaringan sebanding dengan meningkatnya jumlah sentral

yang terpasang. Dengan demikian disamping kurang ekonomis juga relatif mahal dalam pengoperasiannya.

Topologi MESH dibangun dengan memasang banyak link pada setiap komputer. Hal ini dimungkinkan karena pada setiap komputer terdapat lebih dari satu NIC. Topologi ini secara teori memungkinkan akan tetapi tidak praktis dan biayanya cukup tinggi. Topologi Mesh memiliki tingkat redundancy yang tinggi

2.4.5 Topologi Pohon (Tree)

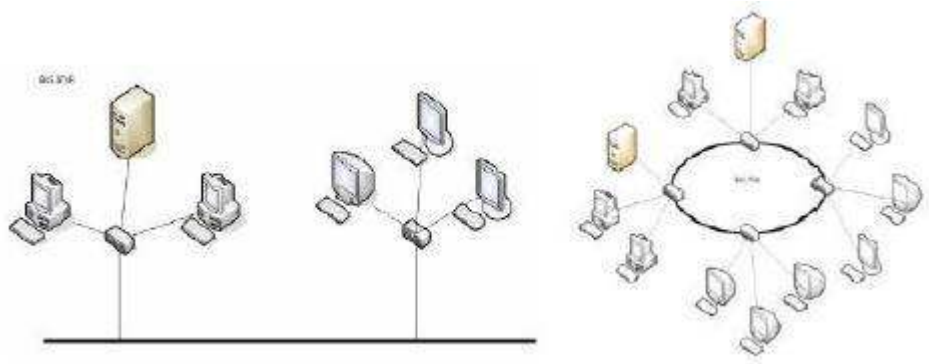


Gambar 2.4.5 Topologi Pohon

Topologi jaringan ini disebut juga sebagai topologi jaringan bertingkat. Topologi ini biasanya digunakan untuk interkoneksi antar sentral dengan hirarki yang berbeda. Untuk hirarki yang lebih rendah digambarkan pada lokasi yang rendah dan semakin keatas

mempunyai hirarki semakin tinggi. Topologi jaringan jenis ini cocok digunakan pada sistem jaringan komputer .

2.4.6 Topologi Hybrid (Campuran)



Gambar 2.4.6 Topologi Hybrid

Topologi Hybrid adalah jaringan yang dibentuk dari berbagai topologi dan teknologi. Sebuah topologi hybrid memiliki semua karakterisitik dari topologi dasar yang terdapat dalam jaringan tersebut.

BAB 3 PEMILIHAN DAN PERANCANGAN PENGUJIAN CAPTIVE PORTAL

Pada bab ini akan dijabarkan urutan proses yang ditempuh dalam sebuah pemilihan software captive portal, jenis dan software captive portal, software-software yang digunakan dalam proses perbandingan, serta perancangan pengujian yang meliputi skema jaringan, lingkungan pengujian dan kriteria evaluasi.

3.1 Proses Pemilihan

Ada beberapa langkah dalam melakukan proses pemilihan captive portal, yaitu:

1. Penentuan software berdasarkan kriteria, proses ini dapat membantu pengguna dalam menentukan captive portal yang sesuai dengan kebutuhan pemakai, pembahasan mengenai hal tersebut dilakukan pada bab tiga.
2. Pemilihan software captive portal yang digunakan dalam proses perbandingan dan pengujian, pembahasan mengenai hal tersebut dilakukan pada bab tiga.
3. Analisis topologi jaringan yang dipergunakan, hal ini dapat membantu dalam pelaksanaan operasional captive portal, pembahasan mengenai hal tersebut dilakukan pada bab tiga.
4. Keunggulan software, telah disebutkan sebelumnya bahwa kriteria menjadi sebuah panduan dalam pemilihan captive portal yang akan dipergunakan, tetapi hal tersebut dapat diimbangi yakni dari aspek lainnya(misalnya berdasarkan kelebihan yang dimiliki setiap software), pembahasan mengenai hal tersebut dilakukan pada bab lima.
5. Implementasi, yakni menerapkan captive portal yang tepat sesuai dengan kebutuhan pengguna, pembahasan mengenai hal tersebut dilakukan pada bab lima.

3.2 Jenis dan Software Captive Portal

Jenis-jenis Captive Portal:

1. Captive portal komersial (berbayar), terdiri atas:
    - software
    - perpaduan antara software dan hardware.
2. Software captive portal (open source).

Berikut ini akan dipaparkan software-software captive portal:

1. Air Marshal, software komersial yang didasarkan untuk platform linux
2. FirstSpot, software komersial dan beroperasi pada sistem operasi windows
3. Mikrotik, komersial berbasis linux
4. Monowall, software captive portal berbasis FreeBSD
5. PfSense, software captive portal berbasis FreeBSD
6. Easy hotspot, software open source berbasis linux

Deskripsi masing-masing captive portal dijelaskan pada tabel 3.2.1.

Tabel 3.2.1 Deskripsi Software Captive Portal

No	Nama Captive Portal	Deskripsi	Fitur	Jenis	Open source/ komersial
1	Air marshal	Air marshal merupakan software captive portal yang tepat untuk digunakan pada lokasi seperti hotel, warnet, universitas, dan area hotspot. Keseluruhan standar berdasarkan dukungan pada radius AAA, hal tersebut memungkinkan air marshal untuk mengintegrasikan dengan fungsi seperti billing dan pengaturan manajemen akses internet.	Radius AAA(authentication, authorized, & accounting), network and session, SSL Encryption, dan masih banyak lagi	Software	komersial
2	FirstSpot	Dalam pengembangan sejak tahun 2002, firstspot® adalah suatu software manajemen wifi hotspot berbasis windows (kadang juga dikenal sebagai software hotspot, pengontrol akses hotspot atau wireless gateway) yang dirancang untuk menjejaki dan mengamankan WiFi hotspot atau area yang membuka akses untuk umum, didasarkan pada teknologi captive portal. Firstspot® mengijinkan para pemakai hotspot untuk masuk dengan menggunakan web browser. Penggunaannya mudah, cepat serta memudahkan proses manajemen hotspot. FirstSpot telah digunakan pada 45 negara dengan 1000 orang pengguna	Pengaturan manajemen hotspot, pengaturan billing hotspot, support banyak bahasa, firewall, load balancing, dan masih banyak lagi.	Software	komersial

No	Nama Captive Portal	Deskripsi	Fitur	Jenis	Open source/ komersial
3	Mikrotik	Mikrotik RouterOS™ adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk IP network dan jaringan wireless, cocok digunakan oleh ISP dan provider hotspot. Meskipun demikian Mikrotik bukanlah perangkat lunak berlisensi bebas, dalam arti untuk menggunakan segala fasilitas yang tersedia pada perangkat lunak ini sejumlah lisensi harus dibeli. Versi uji coba hanya disediakan untuk penggunaan selama 24 jam saja. Perangkat lunak ini tersedia dalam bentuk cakram padat, ataupun DOM (Disk On Module). Khusus untuk versi DOM, perangkat lunak Mikrotik telah terpasang pada modul tersebut sehingga tidak memerlukan instalasi khusus, cukup dengan menancapkan modul DOM tersebut pada slot IDE yang tersedia pada komputer.	Protokoll routing RIP, OSPF, BGP. Pengaturan firewall dan monitoring untuk hotspot melalui winbox GUI, captive portal.	Perpaduan antara software dan hardware.	Komersial
4	Monowall	Monowall adalah sebuah paket firewall yang lengkap dimana ketika digunakan pada embedded PC menyediakan semua fitur penting yang biasanya terdapat pada firewall komersial, termasuk mudah penggunaannya dan tidak berbayar. Monowall dibuat berdasarkan versi FreeBSD yang sejalan dengan web server, PHP dan fungsi lainnya. Keseluruhan konfigurasi sistem disimpan pada satu file teks XML.	Web interface, serial console interface, captive portal, NAT/PAT, dan masih banyak lagi	Software	Open source

No	Nama Captive Portal	Deskripsi	Fitur	Jenis	Open source/ komersial
5	Pfsense	pfsense merupakan software open source yang digunakan sebagai firewall dan router. Memiliki banyak fitur yang dikolaborasikan dengan paket sistem yang dapat digunakan sesuai dengan kebutuhan masing-masing pemgguna, pfsense telah di download oleh 1 juta pendownload. Proyek pembuatan pfsense telah dimulai sejak tahun 2004 sebagai pengembangan dari proyek monowall.	Captive portal, DHCP server dan client, PPTP, IPSEC support, SNMP, dan masih banyak lagi	Software	Open source
6	Easy Hotspot	Easy Hotspot adalah sebuah bundle distro linux berbasis ubuntu 7.10, dipaketkan untuk keperluan hotspot building. Paket itu sudah meliputi tiga komponen yakni membangun hotspot dengan radius AAA (authentication, authorized, & accounting).	Manajemen user, pengaturan voucher, pengaturan voucher, statistik pemantauan pengguna, mengganti password admin, allowed site, secret key.	Software	Open source

Berdasarkan tabel tersebut terdapat tiga buah software captive portal yang digunakan sebagai bahan perbandingan yakni monowall, pfsense, dan easy hotspot. Proses pemilihan software yang dipakai sebagai bahan perbandingan dilihat berdasarkan hal yang telah disebutkan sebelumnya pada batasan masalah, yakni proses pengujian dilakukan pada software captive portal open source.

3.2.1 Monowall

Monowall adalah sebuah paket firewall yang lengkap dan dapat berjalan pada CPU yang memiliki sumberdaya yang terbatas, ketika digunakan pada embedded PC menyediakan semua fitur penting yang biasanya terdapat pada firewall komersial. Termasuk mudah penggunaannya dan tidak berbayar. Monowall dibuat berdasarkan versi FreeBSD 4.11 yang sejalan dengan web server, PHP dan fungsi lainnya. Hasil konfigurasi sistem disimpan pada satu file teks XML. Fitur yang ditawarkan cukup lengkap dan sudah memenuhi kebutuhan untuk dioperasikan sebagai firewall ataupun router untuk internet connection sharing.

Gambar 3.2.1 Tampilan webGUI monowall

Fitur-fitur yang terdapat pada Monowall yakni:

1. web interface (supports SSL) untuk konfigurasi monowall melalui webGUI
2. serial console interface for recovery
    - set LAN IP address
    - reset password
    - restore factory defaults
    - reboot sistem
3. wireless support (access point with PRISM-II/2.5/3 cards, BSS/IBSS with other cards including Cisco)
4. captive portal, untuk mengatur verifikasi pengguna yang akan mengakses jaringan komputer yang terhubung ke internet.
5. stateful packet filtering (firewall), memungkinkan untuk melakukan proses penyaringan IP, IP Protokol, sumber dan tujuan port untuk TCP dan UDP.
    - block / pass rules
    - logging
6. NAT/PAT (including 1:1), penerjemahan alamat private menjadi alamat public dalam mengatur trafik yang menuju dan keluar dari jaringan
7. DHCP client, PPPoE, PPTP and Telstra BigPond Cable support on the WAN interface
8. IPsec VPN tunnels, VPN(virtual private network) memungkinkan pihak tertentu untuk melakukan akses local menggunakan protocol IPsec pada VPN untuk pengamanan transmisi data.
9. PPTP VPN (with RADIUS server support), pengontrolan server dari jarak jauh
10. Static routes, rute statik adalah rute atau jalur spesifik yang ditentukan oleh user untuk meneruskan paket dari sumber ke tujuan. Rute ini ditentukan oleh administrator untuk mengontrol perilaku routing dari IP
11. DHCP server and relay, memberikan IP atau konfigurasi yang diperlukan ketika client memerlukannya.
12. caching DNS forwarder, difungsikan sebagai gateway untuk keperluan proxy internet dan gateway internet.
13. DynDNS client and RFC 2136 DNS updater, memungkinkan admin untuk mendaftarkan IP public untuk memperoleh nama host secara gratis melalui dynamic DNS service provider seperti DynDNS,DHS,dan lain sebagainya.

14. SNMP agent, SNMP (Simple Network Management Protokol) digunakan untuk memonitor perangkat jaringan sehingga dapat memberikan informarsi yang dibutuhkan bagi pengelolanya.
15. Traffic shaper, pembagian atau pengaturan bandwith untuk client.
16. Firmware upgrade through the web browser, memperbaharui generic image monowall versi terbaru melalui web browser.
17. Configuration backup/restore, hasil konfigurasi monowall dapat di ambil dan dipergunakan kembali.
18. Host/network aliases.

Monowall dibuat berdasarkan penggabungan (proses perakitan) dari banyak software, sehingga fitur-fitur yang dimiliki kebanyakan mengambil fungsi dari gabungan software-software, yakni:

1. Semua komponen FreeBSD yang diperlukan (kernel, user programs)
2. IPfilter(firewall)
3. PHP (CGI version)
4. thttpd
5. MPD
6. ISC DHCP server
7. ez-ipupdate (untuk DynDNS update)
8. Dnsmasq (untuk caching DNS forwarder)
9. racoon (untuk IPsec IKE)

Monowall dapat berjalan diberbagai platform seperti live CD, instalasi ke dalam hard disk, embedded di dalam compact flash card. Sistem monowall hanya menghabiskan memori kurang dari 12 MB baik dalam compact flash card maupun pengoperasiannya melalui live CD. Monowall menyediakan beberapa image binary yang bisa didapatkan secara gratis pada situsnya, paket image binary tersebut antara lain:

1. Generic PC/ standard PC untuk proses instalasi ke compact flash card atau hardisk, generic-pc-1.231.img versi terakhir(saat ini)
2. CD-ROM (ISO) image untuk standar PC

Versi monowall:

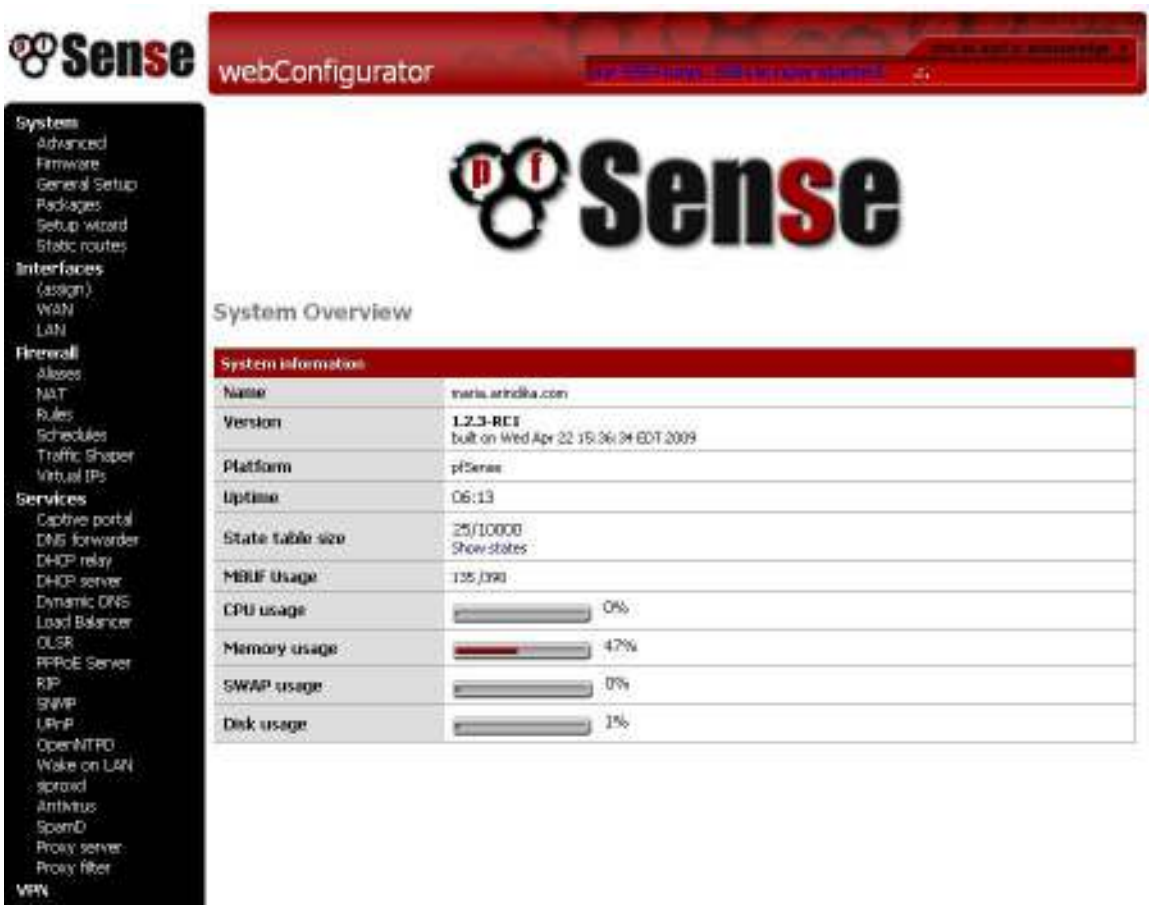
1. PC-Engines WRAP
2. Soekris
3. Generic PC

Spesifikasi komputer yang dibutuhkan untuk membangun Monowall antara lain adalah:

1. Komputer minimal Pentium II, dan memiliki 2 NIC
2. Memori minimal 64 MB
3. Harddisk 40 GB (bisa lebih besar dari itu)

3.2.2 Pfsense

Pfsense merupakan open source firewall yang dibuat berdasarkan pada platform firewall monowall dengan beberapa perbedaan pada fokus penggunaannya. Memiliki paket tambahan yang dapat dipergunakan sesuai dengan kebutuhan pengguna dalam mengatur manajemen hotspot, juga memiliki banyak keunggulan yang biasanya terdapat pada firewall komersial. Pfsense merupakan BSD router yang dibangun berdasarkan pada OS FreeBSD seperti monowall, tetapi menggunakan versi yang berbeda.



Gambar 3.2.2 Tampilan webGUI pfsense

Fitur-fitur yang terdapat pada pfsense merupakan hasil sharing atau mengambil fitur dasar dari monowall, yakni:

1. Captive portal
2. DHCP server and client
3. PPTP, IPSEC support
4. 802.1Q VLAN support, sebuah VLAN Native ditandai dengan sebuah port trunk 802.1Q. Sebuah port trunk 802.1Q mendukung traffic dari banyak VLAN(membagi sebuah broadcast domain yang besar menjadi beberapa broadcast domain yang lebih kecil, tujuannya untuk meningkatkan kinerja jaringan dalam kecepatan pengiriman data). Trunk adalah link point-to point diantara satu atau lebih interface ethernet device jaringan seperti router atau switch.
5. DynDNS client and RFC 2126 DNS updater
6. Caching DNS forwarder

7. SNMP
8. Host/network aliases
9. Configuration backup/restore
10. webGUI
11. upgradable via webGUI
12. Packet filter
13. Multiple WAN support
14. XML, hasil konfigurasi pfsense di simpan pada file XML
15. Load balancing, memungkinkan penggabungan jaringan internet dari dua ISP yang berbeda (multiple WAN support)
16. Traffic shaping, pengaturan bandwith bagi pengguna
17. Package support
18. PPPoE server
19. Themes
20. Setup wizard
21. SSH, protokol standar yang membentuk jalur yang aman pada komunikasi antar komputer untuk login ke server remote (server hosting).
22. Reduced reboots after changes
23. CPU/ Memory / Disk usage meters

Pfsense menyediakan beberapa paket tambahan yang bisa ditambahkan pada sistem pfsense (dapat digunakan sesuai dengan kebutuhan yang dibutuhkan), yakni:

1. Squid (proxy)
2. SpamD, berfungsi untuk mencegah spam
3. Antivirus(clamav+viralator), dan masih banyak lagi.

Pfsense dapat berjalan diberbagai platform seperti pada live CD, instalasi ke dalam hard disk, embedded di dalam compact flash card. Tetapi dalam penggunaan paket tambahan seperti yang telah disebutkan sebelumnya, paket tersebut hanya dapat digunakan jika pfsense di instalasi ke dalam harddisk. Penggunaan pada platform lainnya tidak mendukung ketersediaan paket

tambahan, misalnya pengoperasian pfsense melaui live CD tidak mendukung ketersediaan paket tambahan karena sifatnya yang RO (read only).

Versi pfsense:

1. Versi developer (pengembang pfsense)
2. Embedded PC
3. CD-ROM
4. Instalasi ke dalam hardisk

Spesifikasi komputer yang dibutuhkan:

1. Komputer minimal Pentium I
2. RAM - 128 MB (256 MB atau lebih)
3. Memiliki 2 buah NIC

3.2.3 Easy Hotspot

Easy Hotspot adalah sebuah bundle distro linux berbasis ubuntu 7.10, dipaketkan untuk keperluan hotspot building. Paket itu sudah meliputi tiga komponen yakni membangun hotspot dengan AAA (authentication, authorized, & accounting), tiga komponen tersebut yakni:

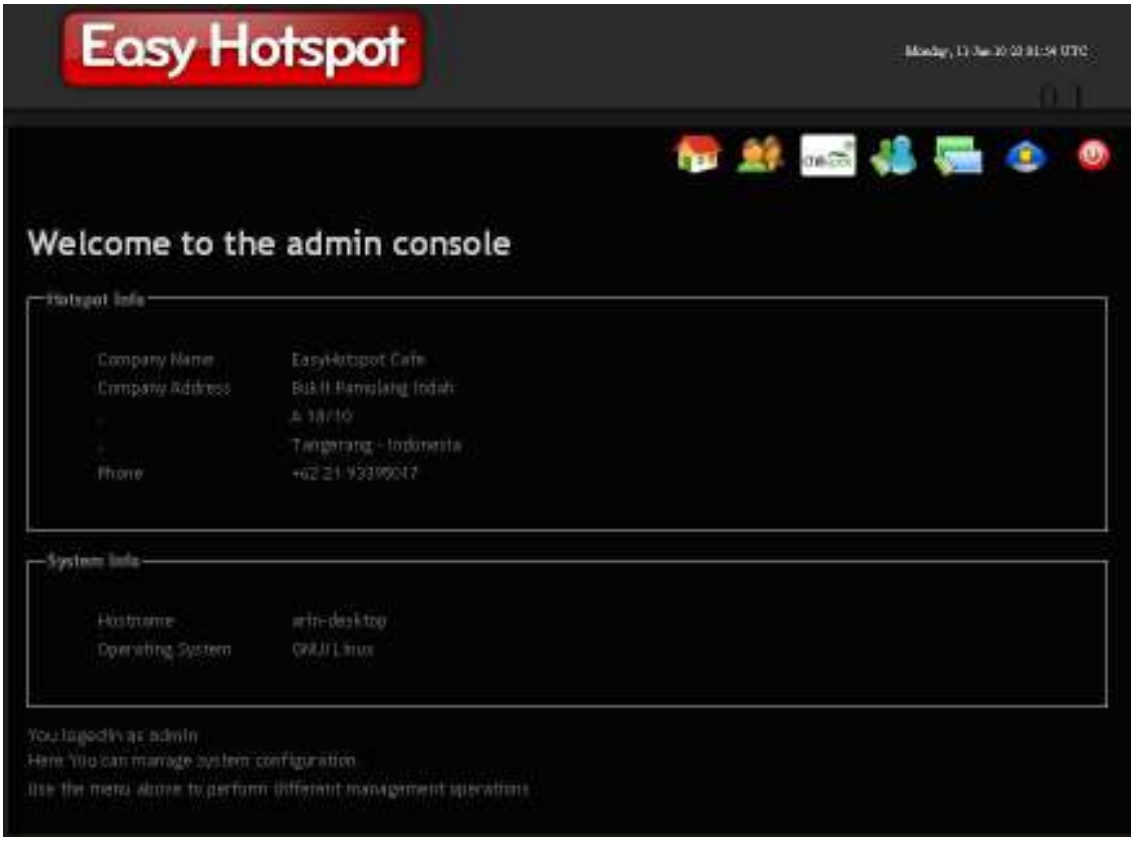
1. **MySql**: Sarana penyimpanan data-data dan informasi-informasi
2. **FreeRadius**: Untuk membangun Radius Server, yaitu merupakan sebuah aplikasi yang memungkinkan keamanan jaringan wireless untuk melakukan authentication, authorize, dan accounting. Selain itu dapat pula untuk mengontrol para pengguna atau user yang ingin mengakses suatu layanan jaringan.
3. **Chillispot:** Adalah captive portal yang di desain untuk authentikasi terhadap database keabsahan user yang sudah ada, seperti RADIUS.

Spesifikasi komputer yang dibutuhkan adalah:

1. Komputer minimal Pentium III

2. 512 MB RAM
3. Minimal harddisk menyisakan area penyimpanan sebesar 5 GB
4. Memiliki 2 NIC

Easyhotspot memiliki pengaturan sistem hotspot dengan menggunakan web interface yang mengatur semua hal yang berhubungan dengan administrasi pemakaian dan aktivitas penagihan. Easyhotspot mempunyai 2 jenis hak akses administrasi yakni kasir dan admin.



Gambar 3.2.3 Tampilan Menu Admin Easy Hotspot

admin : Perencanaan billing, harga dan konfigurasi sistem

kasir : menangani account pengguna, pengaturan voucher, pembuatan invoice

Fitur-fitur yang terdapat pada easy hotspot adalah:

1. Manajemen user
2. Pengaturan voucher (membuat voucher/menghapus voucher).

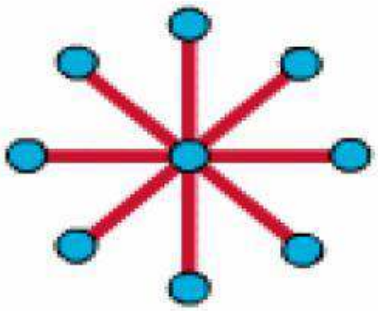
3. Pengaturan billing, prepaid (voucher) dan postpaid (biaya akan dihitung setelah pengguna selesai mengakses internet)
4. Statistik, untuk mengetahui pengguna yang aktif dan pengguna harian.
5. Konfigurasi, untuk mengganti password admin dan pengaturan halaman yang dapat diakses, serta secret key.

3.3 Perancangan Pengujian

Perancangan pengujian dibagi memnjadi tiga proses yakni Skema Jaringan, Lingkungan Pengujian, dan Kriteria Evaluasi.

3.3.1 Skema Jaringan

Captive portal dapat di terapkan pada berbagai jenis topologi jaringan, namun seperti yang telah disebutkan sebelumnya perancangan topologi jaringan akan sangat membantu dalam pelaksanaan operasional captive portal. Salah satu contoh topologi yang dapat dipergunakan adalah topologi star/bintang. Topologi jaringan ini banyak digunakan di berbagai tempat, karena kemudahan untuk menambah, mengurangi atau mendeteksi kerusakan jaringan yang ada. Keuntungan dari topologi ini sangat banyak sekali diantaranya memudahkan admin dalam mengelola jaringan, memudahkan dalam penambahan komputer atau terminal, kemudahan mendeteksi kerusakan dan kesalahan pada jaringan.



Gambar 3.3.1 Topologi Jaringan Star

3.3.2 Lingkungan Pengujian

Tabel 3.3.2.1 Spesifikasi PC Server Monowall

No	Spesifikasi Hardware	
1	Prosesor	Intel(R) Pentium(R) 3 CPU 1.40GHz
2	Memory	512 MB RAM
3	Harddisk	30 GB
4	2 buah NIC	D-Link DFE-530TX+ 10/100BaseTX
		Accton MPX 5030/5030 10/100BaesTX
5	Program utilities	Web browser (mozilla firefox)
6	System operasi	FreeBSD

Tabel 3.3.2.2 Spesifikasi PC Server Pfsense

No	Spesifikasi Hardware	
1	Prosesor	Intel(R) Pentium(R) 4 CPU 2.40GHz
2	Memory	352 MB RAM
3	Harddisk	40 GB
4	2 buah NIC	RealTeak 8139 10/100BaseTX
		VIA VT6102 Rhine II 10/100BaseTX
5	Program utilities	Web browser (mozilla firefox)
6	System operasi	freeBSD

Tabel 3.3.2.3 Spesifikasi PC Server Easy Hotspot

No	Spesifikasi Hardware	
1	Prosesor	Intel(R) Pentium(R) 3 CPU 701.631MHz
2	Memory	512 MB RAM
3	Harddisk	40 GB
4	2 buah NIC	3 Com Corporation 3c905 100BaseTX
		Accton Technology Corporation SMC2-1211TX
5	Program utilities	Web browser (mozilla firefox)
6	System operasi	Linux 7.10

Tabel 3.3.2.4 Spesifikasi PC Client

No	Spesifikasi Hardware	
1	Prosesor	Intel(R) Pentium(R) Dual CPU T3200 @ 2.00GHz (2 CPUs)
2	Memory	1 GB RAM
3	Harddisk	160 GB
4	Sistem operasi	Microsoft windows XP SP 2
5	Program utilities	Web browser (mozilla firefox)

Tabel 3.3.2.5 Spesifikasi PC Router

No	Spesifikasi Hardware	
1	Prosesor	Intel(R) Pentium(R) Dual CPU T3200 @ 2.00GHz (2 CPUs)

2	Memory	Kingston 1978 MB RAM
3	Harddisk	160 GB
4	Sistem operasi	Ubuntu
5	Program utilities	Web browser (mozilla firefox)

Tabel 3.3.2.6 Komponen Pendukung

No	Nama	Deskripsi
1	Kabel UTP RJ-45 tipe straight	Untuk menghubungkan perangkat yang berbeda
2	Kabel UTP RJ-45 tipe crossover	Untuk menghubungkan perangkat yang sama
3	Hub 3Com	Untuk meneruskan signal ke semua port

3.3.3 Kriteria Evaluasi

Dalam pemilihan sebuah software captive portal dapat dilakukan penetapan kriteria secara umum(penetapan sendiri). Kriteria yang dapat digunakan dapat dilihat dari pengukuran terhadap hal-hal tertentu yang diperlukan, walaupun kadang kala kriteria yang ditetapkan oleh pihak yang satu dengan yang lain berbeda. Hal ini dikarenakan perbedaan penggunaan kebutuhan captive portal pada sisi pengguna. Contoh penetapan kriteria menurut Herzog(A Comparison of Open Source ERP Systems, pp:18-27), kriteria yang dipergunakannya untuk membandingkan software ERP yakni :

1. Functional fit
2. Flexibility(customization, flexible upgrades, internationalization, user friendliness, architecture, scalability, security, interfaces, Operating system independence, database independence, programming language)
3. Support(support infrastructure, training, documentation)
4. Continuity(project structure, community activity, transparency, update frequency, other lock in effects)
5. Maturity(development status, reference sites)

Berdasarkan kriteria yang ditetapkan oleh Herzog, dapat pula dilakukan pengacuan kriteria mempergunakan kriteria diatas. Tetapi perlu diketahui bahwa kriteria diatas dipergunakan untuk melakukan perbandingan pada software ERP, yang tentunya memiliki perbedaan dalam penggunaanya karena software ERP digunakan untuk proses bisnis sedangkan software captive portal digunakan untuk manajemen hotspot. Dari kelima kriteria tersebut diketahui masih dibagi

lagi menjadi beberapa sub kriteria, maka dari itu diambil kriteria yang relevan sehingga dapat dipergunakan untuk proses perbandingan pada software captive portal. Dalam hal ini kriteria yang diambil adalah flexibility, support dan continuity. Pengacuan kriteria ini digunakan kembali dalam pemilihan software captive portal untuk mengukur tingkat kemudahan dalam penggunaannya, sedangkan kriteria yang lainnya digabungkan kedalam kriteria yang digunakan. Hasil yang diharapkan dalam proses penelitian ini yakni dapat memberikan acuan/rekomendasi bagi yang akan memanfaatkan software captive portal dalam mengelola wifi hotspot. Untuk penyimpulan hasil perbandingan tersebut dapat diketahui pada proses evaluasi software captive portal .

Berdasarkan proses pendefinisian kriteria, kriteria yang dipergunakan adalah:

1. Kemudahan dalam proses instalasi
    - Fleksibilitas

      Fleksibilitas dijabarkan menjadi sasaran (tujuan) pembuatan software, versi software, support bahasa, user friendly, skalabilitas, keamanan, hardware, bahasa pemograman, OS, proyek software dirilis.

Tabel 3.3.3.1 fleksibilitas

Sasaran(tujuan) pembuatan software	:	mempermudah pengguna dalam mengetahui tingkat kemudahan
versi software	:	Dapat mempermudah pembaharuan versi yang dipergunakan, dengan penambahan yang lebih baik dari sebelumnya
Bahasa yang dipergunakan	:	Dukungan yang diberikan software dalam memberikan support pada berbagai bahasa
User friendly	:	Kemudahan dalam pengoperasiannya
Skalabilitas	:	Kemampuan software secara keseluruhan
Keamanan	:	Firewall
Hardware	:	Kebutuhan spesifikasi hardware yang dibutuhkan
Bahasa pemograman	:	Bahasa yang pakai untuk membangun software tersebut.

OS	:	OS yang dipergunakan sebagai dasar pembuatan software
Proyek software dirilis	:	Pemaparan proyek software tersebut dipublikasikan

- Support

  dijabarkan menjadi support infrastruktur dan dokumentasi (dukungan yang diberikan oleh software tersebut kepada para pengguna software).

Tabel 3.3.3.2 Support

Support infrastruktur	:	Sarana sharing antar pengguna
Dokumentasi	:	Panduan pengoperasian software

- Kesinambungan

  Kesinambungan dijabarkan menjadi status pengembangan(menjelaskan mengenai proses pengembangan software).

Tabel 3.3.3.3 Kesinambungan

Status pengembangan	:	Pengguna memperoleh solusi dalam mengatasi bug yang ada

2. Kemudahan manajemen akses internet berdasarkan voucher.
3. Ketersediaan firewall sebagai keamanan jaringan, dan proxy untuk mempercepat akses client.

BAB 4 IMPLEMENTASI DAN PEMBAHASAN

4.1 Konfigurasi PC Router(Laptop)

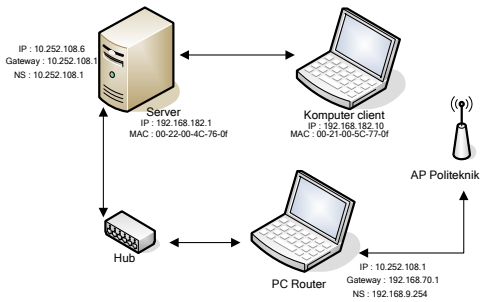
Melakukan konfigurasi untuk menjadikan laptop menjadi mode bridge sehingga menjadi penghubung koneksi wireless internet di lingkungan kampus dengan router Monowall, Pfsense serta Easy Hotspot.

1. Melakukan konfigurasi IP address, netmask, broadcast pada komputer. IP address yang digunakan **10.252.108.1**, netmask **255.255.255.0, dan broadcast 10.252.108.255**
2. Melakukan pengeditan pada file interfaces agar laptop mendapatkan IP DHCP dari wireless AP serta pengarahan pada nameservernya perintahnya adalah **#nano /etc/network/interfaces :**

```
auto lo
iface lo inet loopback

iface eth0 inet static
address 10.252.108.1
netmask 255.255.255.0
auto eth0

#iface eth1 inet dhcp
#auto eth1
```

3. kemudian restart **#sudo /etc/init.d/networking restart**
4. Perintah untuk mengahapus rules yang ada sebelumnya **#iptables -F**
5. Konfigurasi untuk chain NAT, perintahnya adalah **#iptables -t nat -P POSTROUTING ACCEPT, #iptables -t nat -P PREROUTING ACCEPT, #iptables -t nat -P FORWARD ACCEPT**
6. Konfigurasi untuk CHAIN filter, perintahnya adalah **#iptables -P INPUT ACCEPT, #iptables -P FORWARD ACCEPT, #iptables -P OUTPUT ACCEPT**
7. Mejalankan perintah **#iptables -t nat -I POSTROUTING -s 10.252.108.1/24 –j MASQUERADE**

4.2 Implementasi Monowall



Gambar 4.2 Topologi Jaringan Monowall

Berikut ini akan dijabarkan proses konfigurasi monowall:

1. Dalam melakukan konfigurasi monowall dilakukan melalui proses instalasi menggunakan live CD, kemudian akan dilakukan pengaturan pada menu console sebelum dapat melakukan akses pada webGUI monowall di sisi client.
2. Melakukan pengaturan interface, akan ditentukan salah satu NIC yang akan bertindak sebagai LAN dan WAN.
3. Selanjutnya dilakukan pengaturan IP address pada komputer LAN, serta pengaturan DHCP server (untuk memberikan IP address pada client yang terhubung ke server).
4. Melakukan akses webGUI monowall pada komputer client, pada saat hendak melakukan akses pada webGUI monowall masukkan username beserta password sebagai proses identifikasi.
5. Melakukan pengaturan pada webGUI monowall.
6. Pada saat memasuki webGUI monowall dilakukan pemilihan interfaces WAN dengan tipe koneksi static. Masukan alamat IP static yang dipergunakan beserta IP gateway. Melakukan pengaturan pada menu general setup, seperti pemberian nama server yang dibangun, DNS, pemilihan port http/htttps.
7. Melakukan pengaturan captive portal dan pengaturan voucher yang bertujuan untuk memberikan verifikasi pengguna sebelum dapat melakukan akses pada jaringan.
8. Melakukan pengaturan pada firewall (penjelasan mengenai proses implementasi monowall dapat dilihat pada bagian lampiran).

Monowall merupakan firewall, pembuatannya ditujukan untuk embedded PC. Dapat berfungsi sebagai firewall serta difungsikan juga sebagai internet connection sharing. Memiliki beberapa macam versi yang dapat digunakan sesuai dengan kebutuhan pengguna. Penggunaanya support pada satu macam bahasa yakni bahasa inggris. Pengaturannya cukup mudah karena dilakukan melalui WebGUI, dan kemampuannya sangat cepat serta stabil. Cocok digunakan pada komputer yang memiliki spesifikasi hardware yang kecil. Penggunaan HD SATA tidak support, dan memiliki keterbatasan dalam mengenali wireless card dan Ethernet card.

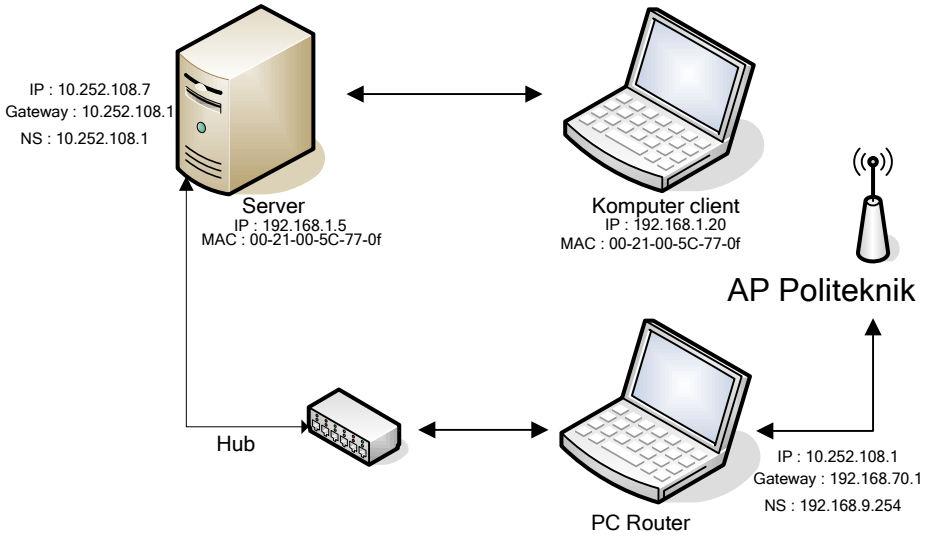
Bahasa pemograman yang digunakan adalah PHP yang digabungkan dengan unsur-unsur lainnya. Selain dapat memanfaatkan software tersebut secara gratis, dapat melakukan pengubahan atau pembaharuan sesuai dengan kebutuhan yang diinginkan. Pengguna juga dapat menikmati layanan komunitas yang berfungsi sebagai sarana diskusi antar pengguna, maupun dengan developer monowall. Forum bagi pengguna monowall dapat dikunjungi pada situs http://**forum**.m0n0.ch/. Monowall mailing list dapat dikunjungi pada situs http://m0n0.ch/wall/list/. Untuk mempermudah penggunaan software tersebut, terdapat buku panduan monowall yang dapat diperoleh secara gratis pada situs http://doc.m0n0.ch/handbook-single/. Software ini tidak memiliki pengaturan proxy, dirilis pada bulan februari 2003 dan dibuat berdasarkan versi FreeBSD versi 4.1.1.

Tabel 4.2.1 Evaluasi Monowall

Monowall		
Kemudahan instalasi		
1	Fleksibilitas	
	Sasaran(tujuan) pembuatan	Embedded PC, Monowall di buat sesimpel mungkin, fungsi-fungsi yang tidak diperlukan (fungsi dasar yang dimilikipada OS FreeBSD) ditiadakan.
	Versi software	PC engine-WRAP, Soekris, Generic PC
	Bahasa yang dipergunakan	Inggris
	User friendly	Pengaturan dari menu console dan webGUI
	Skalabilitas	Sangat cepat dan stabil
	Keamanan	firewall NAT/PAT(1:1)
	Hardware	Cocok digunakan pada komputer yang memiliki spesifikasi yang kecil, penggunaan HD SATA tidak support, wireless card dan Ethernet card yang dikenali terbatas.
	Bahasa pemograman	PHP dan gabungan perangkat lunak lainnya
	OS	Dibuat berdasarkan OS FreeBSD 4.11
	Proyek dirilis	Februari 2003
2	Support	
	Support infrastruktur	Forum, mailling list, IRC channel
	Dokumentasi	Monowall manual handbook
3	Kesinambungan	
	Status pengembangan	Terus mengalami pembaharuan/update pada berbagai versi yang dimiliki
Manajemen akses		Bentuk pengaturan voucher sangat baik, dapat

berdasarkanvoucher	membuat paket voucher untuk aktifasi pada waktu yang ditentukan dalam satu paket
Firewall	Rules, NAT, traffic shaper, aliases
Proxy	tidak memiliki pengaturan proxy

4.3 Implementasi Pfsense



Gambar 4.3 Topologi jaringan Pfsense

Berikut ini akan dijabarkan proses konfigurasi pfsense:

1. Untuk pengoperasian pfsense dilakukan melalui proses instalasi ke dalam harddisk menggunakan live cd, kemudian akan dilakukan pengaturan interface LAN dan WAN, serta pengaturan IP address LAN pada menu console.
2. Untuk pengaturan interface harus ditentukan terlebih dahulu salah satu NIC yang akan bertindak sebagai LAN dan WAN.
3. Selanjutnya dilakukan pengaturan IP address pada komputer server, serta pengaturan DHCP server (untuk memberikan IP address pada client yang terhubung ke server).
4. Setelah semua proses dilakukan langkah selanjutnya adalah melakukan akses pada webGUI monowall pada komputer di sisi client, maka akan ditampilkan permintaan untuk memasukan username beserta password sebagai proses identifikasi.
5. Pada saat memasuki webGUI pfsense pilihlah interfaces WAN dengan tipe koneksi yang akan dipergunakan misalnya static.

6. Kemudian lakukan pengaturan pada captive portal dan user yang dapat melakukan akses internet(dalam pengoperasian pfsense versi 1.2.3-RC1 tidak memiliki pengaturan voucher) sebagai proses verifikasi pengguna yang hendak terhubung pada jaringan.
7. Melakukan pengaturan firewall yang dapat digunakan misalnya untuk membatasi akses pengguna pada situs-situs tertentu.
8. Melakukan instalasi package yang hendak dipergunakan (penjelasan mengenai proses implementasi pfsense dapat dilhat pada lampiran).

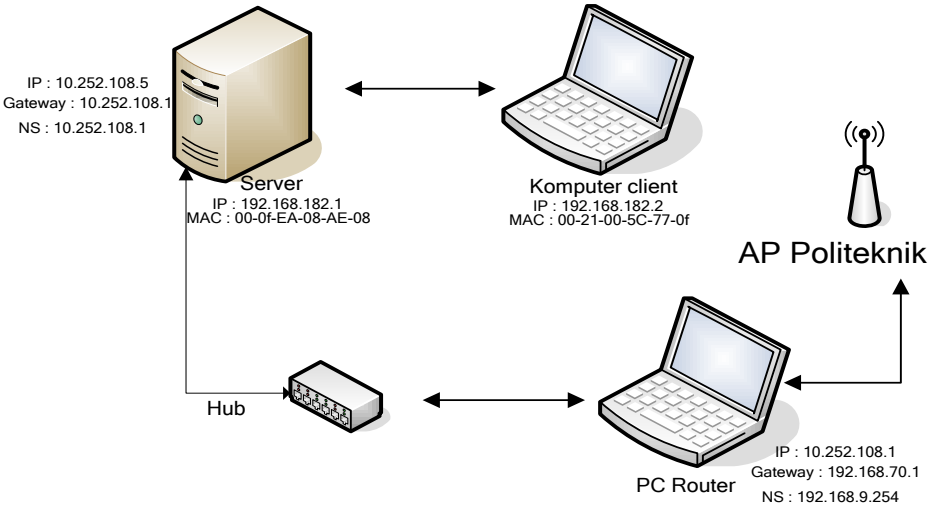
Pfsense merupakan firewall, penggunaannya tidak ditujukan untuk embedded PC. Dapat di fungsikan untuk pengaturan internet connection sharing. Memiliki beberapa macam versi yang dapat digunakan sesuai dengan pemakaian pengguna. Penggunaanya memberikan support pada satu macam bahasa yakni bahasa inggris. Pengaturannya cukup mudah karena dilakukan melalui WebGUI seperti monowall(pfsense merupakan software turunan dari monowall). Kemampuannya sangat cepat dan stabil, cocok digunakan pada berbagai tipe wireless card.

Bahasa pemograman yang digunakan adalah PHP yang digabungkan dengan unsur-unsur lainnya. Pengguna selain dapat memanfaatkan software tersebut secara gratis, dapat pula melakukan pengubahan atau pembaharuan sesuai dengan kebutuhan yang diinginkan. Pengguna juga dapat menikmati layanan komunitas yang berfungsi sebagai sarana diskusi antar pengguna, maupun dengan developer monowall. Forum bagi pengguna monowall dapat dikunjungi pada situs http://forum.pfsense.org/index.php/topic,18823.0.html. Pfsense mailing list dapat dikunjungi pada situs http://www.pfsense.org/index.php?option=com_content&task=view&id=66&Itemid=71. Penggunaan pfsense tidak dilengkapi dengan buku panduan(manual handbook), tetapi pengguna dapat memperoleh tutorial penggunaan pfsense yang dibuat oleh para pengguna pfsense lainnya. Situsnya dapat dikunjungi pada http://doc.pfsense.org/index.php/Tutorials. Software ini memiliki pengaturan proxy, dirilis pada bulan November 2004 dan dibuat berdasarkan versi FreeBSD versi 6.1.

Tabel 4.3.1 Evaluasi Pfsense

Pfsense		
Kemudahan instalasi		
1	Fleksibilitas	
	Sasaran(tujuan) pembuatan	Pembuatannya tidak difokuskan untuk versi embedded. Merupakan software pengembangan dari monowall(memiliki fitur-fitur yang sama dengan penambahan pada fungsi package yang dapat dipergunakan sesuai dengan kebutuhan pengguna). Dibuat untuk mengoptimalkan kinerja hardware. Pfsense di buat berdasarkan OS FreeBSD.
	Versi software	Versi developer edition, embedded, CD-ROM, full instalasi
	Bahasa yang dipergunakan	Inggris
	User friendly	Pengaturan dari menu console dan webGUI
	Skalabilitas	Sangat bagus
	Keamanan	firewall NAT/PAT(1:1)
	Hardware	Support penggunaan berbagai macam wireless card terutama atheros
	Bahasa pemograman	PHP dan gabungan perangkat lunak lainnya
	OS	Dibuat berdasarkan OS FreeBSD 6.1
	Proyek dirilis	November 2004
2	Support	
	Support infrastruktur	800 orang terdaftar dalam forum (bertambah 4 user baru per harinya), lebih dari 400 mailling list, IRC channel beranggotakan sekitar 80 orang
	Dokumentasi	Terdapat tutorial yang dibuat secara manual oleh para pengguna pfsense, manual handbook pfsense yang diperjual belikan pada situs www.amazon.com.
3	Kesinambungan	
	Status pengembangan	Terus mengalami pembaharuan pada berbagai versi yang dimiliki
Manajemen akses berdasarkan voucher		Untuk pfsense versi 1.2.3-RC1 tidak memiliki pengaturan voucher
Firewall		Aliases, NAT, Rules, schedules, traffic shaper, virtual IPs
Proxy		Memiliki pengaturan proxy. Server menyimpan halaman cache web sebelumnya, sehingga bila ada permintaan ulang terhadap halaman web tersebut dapat dimunculkan kembali dalam waktu singkat.

4.4 Implementasi Easy Hotspot



Gambar 4.4 Topologi jaringan Easy Hotspot

Berikut ini akan dijabarkan proses konfigurasi easy hotspot:

1. Untuk pengoperasiannya dilakukan instalasi easy hotspot ke dalam harddisk
2. Melakukan identifikasi pada ethernet card. Jika ethernet card yang terlihat adalah eth3 dan eth4, maka harus dilakukan pengubahan supaya ethernet card menjadi eth0 & eth1. Perintahnya adalah **#vim /etc/udev/rules.d/70-persistent-net.rules**
3. Melakukan pengaturan agar eth0 sebagai terkoneksi menuju jaringan luar, perintahnya adalah **#ifconfig eth0 10.252.108.5 netmask 255.255.255.0**
4. Perintah untuk mengarahkan ke IP gateway adalah **#route add default gw 10.252.108.1**
5. Membuat nameserver, perintahnya adalah **#echo "nameserver 10.252.108.1" > /etc/resolv.conf**
6. Menghubungkan komputer client dengan komputer server, dan mengatur komputer client agar memperoleh alamat IP secara otomatis.
7. Melakukan pengaturan voucher berupa sistem perhitungan prepaid.

Easy Hotspot merupakan salah satu distro ubuntu yang dibuat untuk keperluan hotspot building, versi yang dimiliki untuk saat ini yakni **0.1** dan **0.2**. Memberikan support pada beberapa bahasa seperti inggris, Indonesia dan Spanish. Penggunaanya cukup mudah yakni

melalui webGUI. Sakalabilitasnya cukup baik. Memiliki pengaturan firewall. Bahasa pemograman yang digunakan untuk membuat software ini terdiri dari PHP dan gabungan dari berbagai perangkat lunak lainnya. Pengguna software ini juga dapat bertukar pikiran mengenai setiap permasalahan yang dihadapi, seperti adanya bug maupun dalam proses pengoperasiannya melalui blog pembuat easy hotspot. Dokumentasi yang disediakan berupa tutorial yang dapat mempermudah pengoperasian easy hotspot, dapat dilihat pada situs http://easyhotspot.sourceforge.net. Untuk pengaturan koneksi internet dapat dilakukan pengaturan berupa prepaid dan postpaid management. Untuk pengaturan proxy tidak dimiliki oleh easyhotspot, dan bila pengguna hendak memanfaatkannnya harus dilakukan proses instalasi proxy secara manual.

Tabel 4.4.1 Evaluasi Easy Hotspot

Easy hotspot		
Kemudahan instalasi		
1	Fleksibilitas	
	Sasaran(tujuan) pembuatan	Paket Hotspot building dengan penggunaan yang lebih mudah
	Versi software	Versi 0.1, versi 0.2
	Bahasa yang dipergunakan	English, Indonesia, spanish
	User friendly	Pengaturan dari webGUI dan terminal
	Skalabilitas	Baik
	Keamanan	Firewall
	Hardware	Penggunaannya dibutuhkan komputer dengan spesifikasi yang lebih besar
	Bahasa pemograman	PHP dan gabungan perangkat lunak lainnya
	OS	Ubuntu 7.10
	Proyek dirilis	-
2	Support	
	Support infrastruktur	blog pendiri easy hotspot
	Dokumentasi	Dokumentasi easy hotspot berupa tutorial dapat dilihat pada situs easy hotspot
3	Kesinambungan	
	Status pengembangan	Terus mengalami pembaharuan
Manajemen akses berdasarkan voucher		Bentuk pengaturan voucher sangat baik. Pengaturan Postpaid dibagi berupa time based dan volume based
Firewall		Tersedia
Proxy		Pengguna dapat menambahkan squid untuk proxy

4.5 Perbandingan Monowall, Pfsense dan Easy Hotspot

Tabel 5.1.1 Kesimpulan

Kriteria Evaluasi		Captive Portal Open Source		
	Sub Kriteria	Monowall	Pfsense	EasyHotspot
Fleksibilitas				
	Sasaran(tujuan) pembuatan	embedded PC	Instalasi pada PC	Instalasi pada PC
	Versi software	PC engine-WRAP, Soekris, Generic PC	developer edition, embedded, CD-ROM, full instalasi	Versi 0.1, versi 0.2
	Bahasa yang dipergunakan	Mendukung satu macam bahasa	Mendukung satu macam bahasa	Mendukung lebih dari satu bahasa
	User friendly	Pengaturan berbasis webGUI	Pengaturan berbasis webGUI	Pengaturan masih dilakukan secara manual
	Skalabilitas	Sangat cepat dan stabil	Sangat bagus	Baik
	Keamanan	firewall NAT/PAT(1:1)	firewall NAT/PAT(1:1)	Firewall
	Hardware	komputer dengan spesifikasi yang kecil,	Support penggunaan berbagai macam wireless card	komputer dengan spesifikasi yang besar
		SATA tidak support,	terutama atheros, komputer dengan spesifikasi yang besar	
		wireless card dan Ethernet card yang dikenali terbatas		
	Bahasa pemograman	PHP dan gabungan perangkat lunak lainnya	PHP dan gabungan perangkat lunak lainnya	PHP dan gabungan perangkat lunak lainnya
	OS	FreeBSD 4.11	FreeBSD 6.1	Ubuntu 7.10
	Proyek dirilis	Februari 2003	11/1/2004	-
Support				
	Support infrastruktur	Forum, mailling list, IRC channel	Forum, mailling list, IRC channel	blog
	Dokumentasi	Monowall manual handbook	pfsense tutorial	easy hotspot tutorial
Kesinambungan				
	Status pengembangan	Terus mengalami pembaharuan	Terus mengalami pembaharuan	Terus mengalami pembaharuan
Manajemen akses berdasarkan voucher		tersedia	tersedia	tersedia
Firewall		tersedia	tersedia	tersedia
Proxy		tidak ada	tersedia	Dapat di lakukan penambahan proxy
Kelebihan		difungsikan sebagai router dan pengaturan internet	difungsikan sebagai router dan pengaturan internet	difungsikan untuk mengatur billing hotspot
		Penggunaan voucher tidak terpengaruh pada koneksi	terdapat fitur-fitur tambahan	dapat dilakukan instalasi untuk aplikasi lain
		mempergunakan port https	terdapat antivirus dan konfigurasi untuk multiple uplink	mempergunakan port https
		digunakan pada jaringan yang besar dan kecil	mempergunakan port https	
		memiliki pengaturan traffic shaper	digunakan pada jaringan yang besar dan kecil	
			memiliki pengaturan traffic shaper	
Kekurangan		dalam pembuatan voucher, terjadi voucher ganda		digunakan pada jaringan yang kecil
		tidak difungsikan untuk pengaturan billing hotspot	tidak difungsikan untuk pengaturan billing hotspot	Penggunaan voucher dipengaruhi oleh koneksi
			Masih terdapat error/kesalahan	

Penyimpulan hasil evaluasi dari proses implementasi dan pembahasan yang dibuat berdasarkan tabel 5.1.1:

1. Monowall lebih baik dari segi penggunaan resource komputer, karena tidak mengambil kapasitas yang terlalu besar yakni 6 MB embedded didalam CF card. Sedangkan dua software lainnya mengambil kapasitas resource PC dalam jumlah yang besar.
2. Pada penggunaan voucher monowall jika koneksi pengguna terputus disebabkan oleh faktor tertentu sedangkan waktu pemakaian voucher belum habis, maka pengguna dapat meneruskan pemakaian koneksi internet.
3. Dalam proses pembuatan voucher pada monowall terjadi voucher ganda, walaupun dibuat dalam durasi waktu yang berbeda. Hal ini menyebabkan pengguna tidak bisa melakukan akses internet dikarenakan voucher tersebut telah digunakan sebelumnya.
4. Monowall dan pfsense memiliki fitur-fitur yang sama, perbedaannya terletak pada ketersediaan pfsense terhadap fitur-fitur tambahan yang dapat digunakan sesuai dengan kebutuhan.
5. Fitur-fitur yang terdapat pada monowall dan pfsense cukup banyak, walaupun tidak semua fitur dipakai(tergantung kebutuhan). Fitur-fitur yang terdapat pada pfsense cukup membingungkan penggunaannya bagi pengguna hal ini dikarenakan tidak tersediannya manual handbook sebagai panduan dalam pengoperasian pfsense, fitur-fitur yang terdapat pada easy hotspot pengoperasiannya cukup mudah dan tidak terlalu sulit.
6. Jika monowall dan pfsense di atur sedemikian rupa agar menggunakan protocol https, ketika dilakukan proses restart tidak dapat menampilkan webGUI(walaupun kondisinya client memperoleh IP, dan alamat IP tersebut ketika di ping memberikan respon).
7. Keunggulan pfsense dibanding monowall yakni tersedianya squid proxy, antivirus scan, serta konfigurasi untuk multiple uplinks(load balancing)
8. Pada saat melakukan pengujian menggunakan pfsense versi developer, masih ditemukan adanya error/kesalahan sehingga webGUI pfsense tidak dapat terakses dengan baik(pfsense memiliki fitur yang paling lengkap dari semua software yang diuji).
9. Easy hotspot dikhususkan untuk management hotspot beserta billing akses internet, namun masih dapat juga dilakukan instalasi aplikasi lainnya seperti halnya distro linux yang lain.

10. Dalam pemanfaatan voucher pada software easy hotspot jika koneksi pengguna terputus atau diputus, sedangkan waktu pemakaian voucher belum habis, maka pengguna tidak dapat meneruskan pemakaian koneksi internet. Hal ini menyebabkan pengguna harus memperoleh voucher yang baru.
11. Kemampuan easyhotspot sangat baik dimana proses verifikasi pengguna menggunakan port https sehingga data verifikasi menjadi terenkripsi, bila terjadi aktifitas sniffing aktifitas tersebut menjadi tidak berguna. Easy hotspot sendiri sangat cocok digunakan untuk membangun jaringan warnet kabel maupun nirkabel.
12. Perbedaan antara monowall, pfsense dan easyhotspot yakni terletak pada proses pengaturan. Untuk konfigurasi easyhotspot masih dilakukan pengetikan secara manual, sedangkan pada monowall dan easyhotspot pengaturannya menjadi lebih mudah karena menggunakan webGUI.
13. Berdasarkan proses pembahasan yang telah dibahas pada bab 4, fleksibilitas paling baik dimiliki oleh easyhotspot.
14. Berdasarkan proses pembahasan yang telah dibahas pada bab 4, support paling baik diberikan oleh pfsense
15. Ketiga software yang digunakan dalam proses perbandingan untuk saat ini masih memperoleh dukungan kesinambungan dari pihak developer masing-masing software.
16. Netcut dapat diatasi dengan melakukan block pada IP address komputer yang melakukan aksi tersebut, selain itu dapat dilakukan pengaturan bandwith menggunakan fasilitas traffic shaper seperti yang terdapat pada software monowall dan pfsense

BAB 5 KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan yang dapat diambil berdasarkan proses perbandingan software captive portal adalah:

1. Proses pemilihan software captive portal dapat dipergunakan sesuai dengan kebutuhan pengguna
    - Monowall dan pfsense dapat dipergunakan jika pengguna hendak membangun sebuah PC router yang handal yang memiliki pengaturan firewall, dan dapat juga dipergunakan untuk pengaturan internet connection sharing. Memiliki fitur-fitur yang lebih kompleks, penggunaan software tersebut cocok diterapkan pada jaringan kecil maupun besar.
    - Easy hotspot dapat dipergunakan jika pengguna hendak membangun suatu server billing hotspot untuk akses internet, penggunaannya cocok pada warnet dan cafe.

2. Berdasarkan tujuan penelitian, telah dilakukan pencapaian untuk mengetahui kelebihan dan kelemahan yang terdapat dalam software captive portal, serta menyimpulkan hasil evaluasi proses perbadingan software captive portal yang dapat dipergunakan sebagai acuan dalam pemilihan sebuah software captive portal.

3. Untuk melakukan perbadingan software captive portal dilakukan penetapan kriteria yang dipergunakan sebagai pembanding dalam pemilihan software yakni:
    - Kemudahan dalam proses instalasi.
    - Kemudahan manajemen akses internet berdasarkan voucher.
    - Ketersediaan firewall sebagai keamanan jaringan, dan proxy untuk mempercepat akses client.

5.2 Saran

Adapun saran untuk pengembangan dalam proses perbandingan selanjutnya adalah :

1. Pengujian dari sisi keamanan jaringan pada software-software captive portal dilakukan hanya terbatas pada pengujian berupa aktifitas sniffing username dan password, belum diketahui kemampuan software tersebut dalam menangulangi serangan DDos, session hijacking dan lainnya.
2. Untuk mengetahui performa masing-masing software, dapat dilakukan pengujian pada berbagai bentuk topologi jaringan komputer.
3. Kriteria evaluasi yang dipergunakan dapat ditambahkan misalnya kemampuan monitoring segala aktifitas yang terjadi di dalam jaringan.
4. Pada proses pengujian terdapat kendala dalam melakukan pengujian pada keseluruhan fitur yang ada pada software captive portal karena keterbatasan fasilitas yang diperlukan.

DAFTAR PUSTAKA

1. EasyHotspot documentation beserta software , (2009, Desember). Tersedia : http://www.easyhotspot.sourceforge.net
2. Hacker friendly LLC, ”Jaringan Wireless di Dunia Berkembang”, (2007, Desember). Tersedia : http://hackerfriendly.com/
3. Kasper, Manuel, “M0n0wall Handbook”, (2005, September). Tersedia : http://doc.m0n0.ch/handbook-single/
4. The open source definition, (2009, Desember). Tersedia : http://www.opensource.org/
5. I. Suardika, P. Warma, and N. Fitriani, “Memilih Topologi Jaringan dalam Mendesain Suatu Jaringan Komputer”, bali 2007, pp. 1–5.
6. Herzog, Thomas, “A Comparison of Open Source ERP Systems” , Institute of Information Systems and Operations, Department of Business Management and Information Systems Vienna University of Economics and Business Administration, Vienna, Juni.2006, pp. 18-27
7. Software pfsense,(diakses 11 september 2009) Tersedia : http://www.pfsense.org/
8. Software monowall, (diakses 05 september 2009) Tersedia: http://**www**.m0n0.ch/.
9. Cain & Abel, (diakses 07 september 2009) Tersedia: http://www.oxid.it/cain.html.

LAMPIRAN PROSES IMPLEMENTASI

Berikut ini akan dilakukan pembahasan mengenai proses konfigurasi pada tiga buah software captive portal.

1.1 Monowall

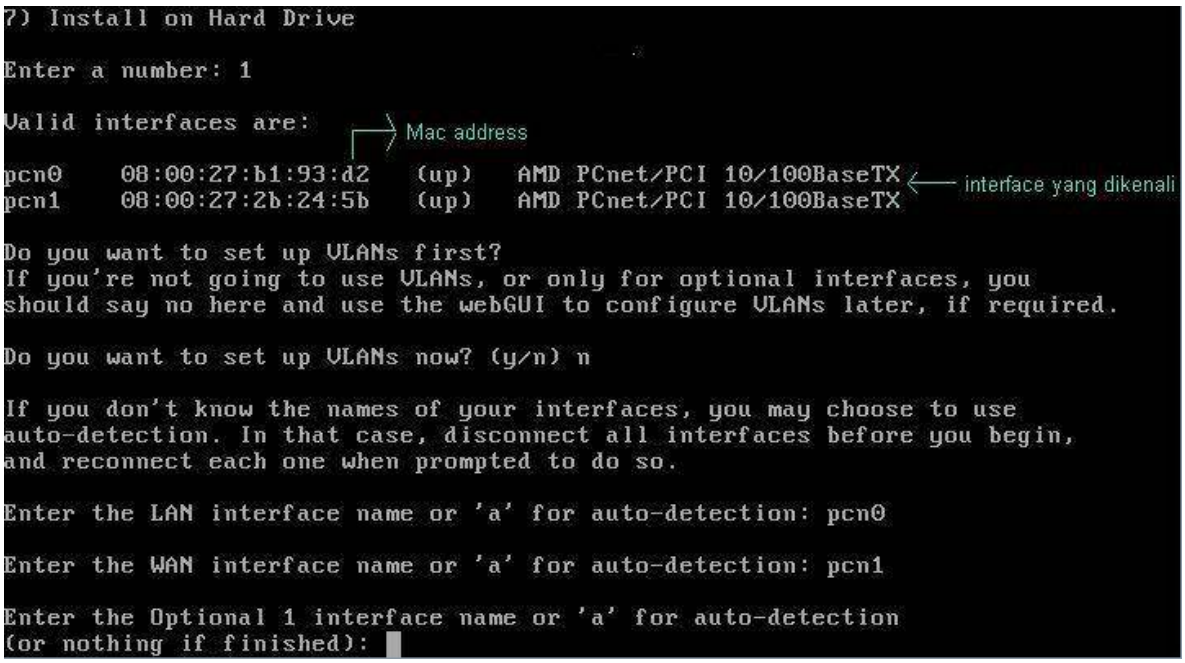
Seperti yang telah disebutkan sebelumnya konfigurasi monowall dilakukan melalui proses instalasi kedalam harddisk melalui live CD. Berikut ini akan dipaparkan langkah-langkah untuk mengkonfigurasi interface (NIC) yang terhubung ke LAN sebagai langkah pendahuluan sebelum mengkonfigurasi IP address dan administrasi monowall lebih lanjut dengan webGUI. Sebelum hendak mengkonfigurasi interface (NIC) terlebih dahulu akan dilakukan pembahasan mengenai menu console setup seperti yang tampak pada gambar berikut.

Menu console setup digunakan untuk konfigurasi dasar sistem, dimana terdapat lima menu yang masing-masing mempunyai fungsi seperti berikut:

- Interface : assign network ports, menu ini digunakan untuk mendefinisikan ethernet card(NIC) yang digunakan.

- Set up LAN IP address, digunakan untuk melakukan pengaturan IP address ethernet card yang terhubung ke jaringan lokal(LAN).
- Reset webGUI password, digunakan jika ingin melakukan pengubahan username dan password yang secara default terdapat pada monowall
- Reset to factory defaults, untuk mengembalikan ke konfigurasi awal seperti ketika baru menginstall.
- Reboot system, untuk merestart system.
- Ping host, untuk melakukan ping ke host/komputer tertentu dan juga bisa di gunakan untuk melakukan test koneksi ke host lain.

Berdasarkan gambar diatas secara default monowall mendefinisikan network interface(NIC) dengan nama sis0, sis1, …, sisx. Jika terdapat lebih dari satu interface maka monowall akan mendefinisikan sis0(sis nol) untuk interface LAN dan sis1(sis satu) untuk interface WAN(jaringan luar/internet) yang ditampilkan pada bagian Port Configuration, tepatnya diatas menu console setup pada saat pertama kali loading. Penggunaan konfigurasi interface(sis0/sis1) default monowall dan langsung mengkonfigurasi IP address LAN akan membuat koneksi gagal, maka diperlukan pendefinisian ulang interface tersebut.



Pada bagian "Enter a number:" masukan angka satu (Interface: assign network port) dan tekan enter. Maka monowall akan menampilkan semua interface yang valid beserta MAC addressnya sebagai acuan untuk menetukan interface yang digunakan untuk

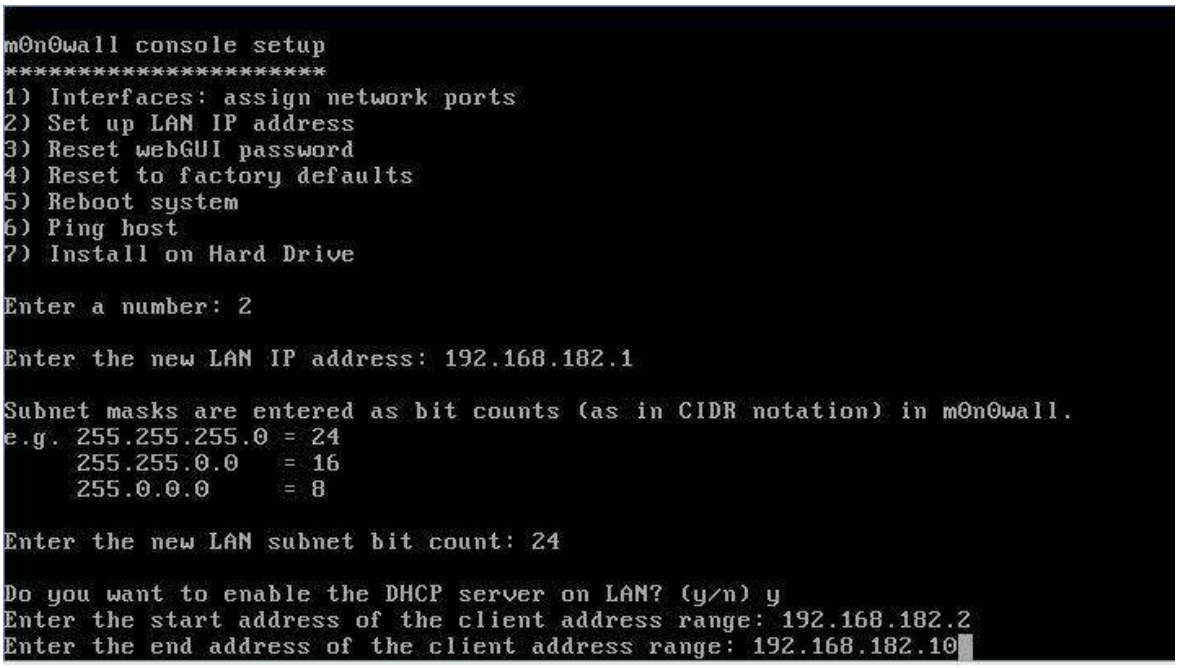
LAN/WAN, disini monowall mengenali dua buah interface yang ada pada komputer yaitu pcn0 dan pcn1.

kemudian tampil pertanyaan yang menanyakan apakah kita ingin melakukan pengaturan VLANs, untuk sementara jawablah tidak dengan memasukan huruf ‘n’ dan tekan enter. Setelah itu akan muncul dialog agar memasukan nama interface yang di gunakan untuk koneksi ke jaringan lokal (LAN) dan interface untuk WAN. Pada contoh kasus ini interface yang terhubung ke LAN adalah pcn0 dan interface yang terhubung ke WAN/internet adalah pcn1. Setelah memasukan interface untuk WAN akan muncul pertanyaan apakah kita akan memasukan interface tambahan(lihat gambar diatas), karena yang digunakan disini hanya dua interface maka biarkan kosong dan tekan enter. Selanjutnya monowall akan menampilan report untuk interface yang telah ditetapkan dan menanyakan apakah hendak dilakukan pemrosesan, tekan 'y' kemudian enter untuk memprosesnya, kemudian monowall akan melakukan restart pada computer sehingga bisa dilakukan konfigurasi selanjutnya yaitu konfigurasi IP address untuk interface LAN agar bisa diakses melalui webGUI untuk administrasi lebih lanjut.

```
Do you want to set up VLANs first?
If you're not going to use VLANs, or only for optional interfaces, you
should say no here and use the webGUI to configure VLANs later, if required.

Do you want to set up VLANs now? (y/n) n

If you don't know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces before you begin,
and reconnect each one when prompted to do so.

Enter the LAN interface name or 'a' for auto-detection: pcn0

Enter the WAN interface name or 'a' for auto-detection: pcn1

Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:

LAN  -> pcn0
WAN  -> pcn1

The firewall will reboot after saving the changes.

Do you want to proceed? (y/n) y
```

Setelah konfigurasi interface selesai berikutnya adalah pemberian IP address untuk interface LAN, secara default monowall memberi IP address untuk interface LAN dengan 192.168.1.1. Semetara untuk konfigurasi IP address interface WAN dilakukan melalui webGUI karena di console setup tidak tersedia menu untuk konfigurasi IP address WAN.

Agar bisa mengakses webGUI dari monowall terlebih dahulu kita harus mengkonfigurasi IP address LAN, untuk melakukannya kita menggunakan menu console setup nomor dua(Set up LAN IP address).

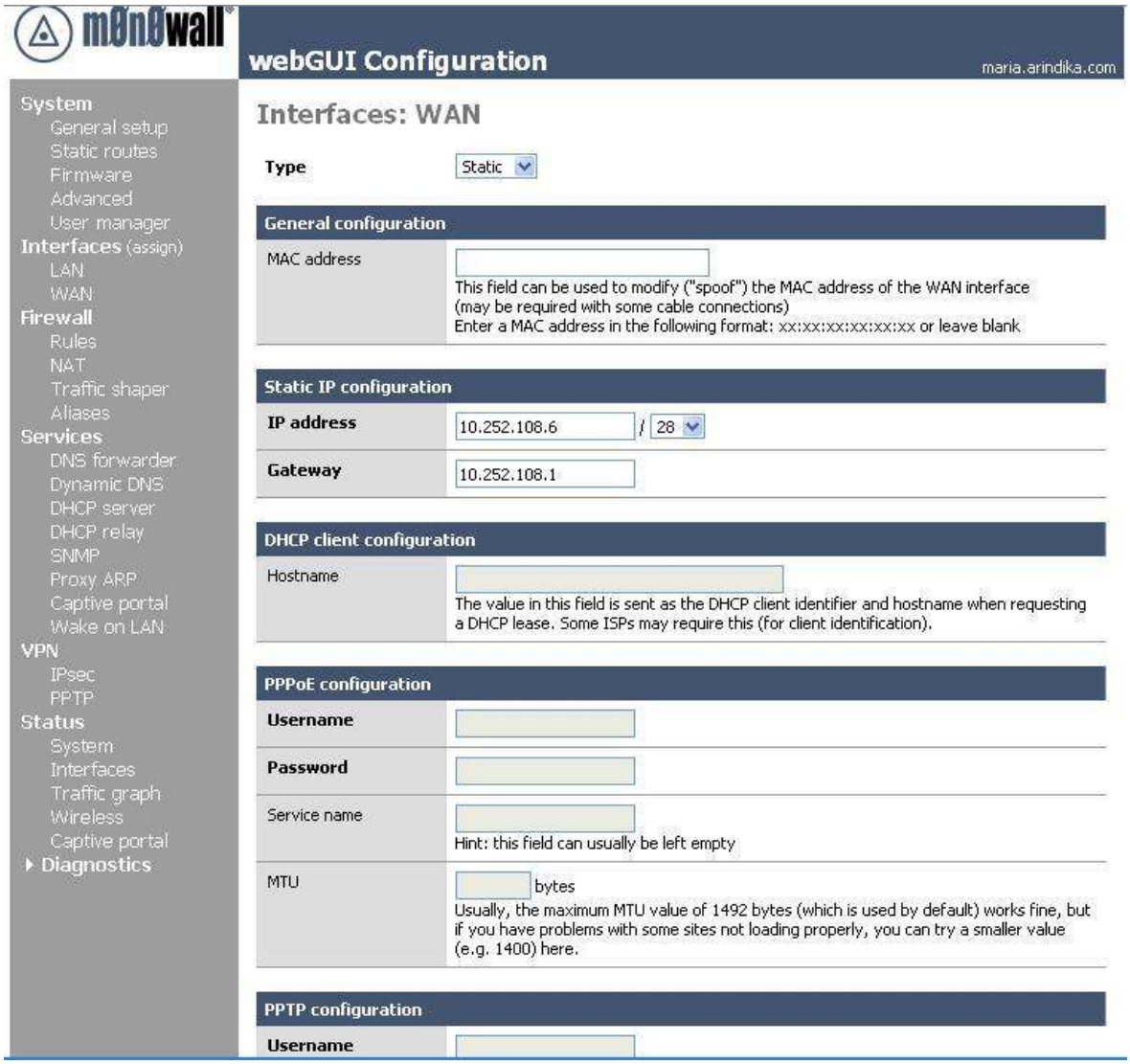


Di console setup di bagian "Enter Number:' masukan angka 2 dan kemudian tekan enter, selanjutnya masukan IP address untuk LAN, kemudian memasukan subnetmask, karena IP address yang kita gunakan adalah kelas C(192.168.xxx.xxx) dimana secara default netmasknya adalah 255.255.255.0 atau 24 yang dapat memuat 254 host, selanjutnya akan muncul pertayaan apakah kita akan mengaktifkan DHCP server agar komputer client di LAN mendapatkan IP address otomatis, tekan ‘y’ untuk aktifasi DHCP server kemudian tekan enter, setelah mengaktifkan DHCP server kemudian harus memasukan rentang IP Address yang di alokasikan bagi komputer klien untuk mendapatkan IP address otomatis.

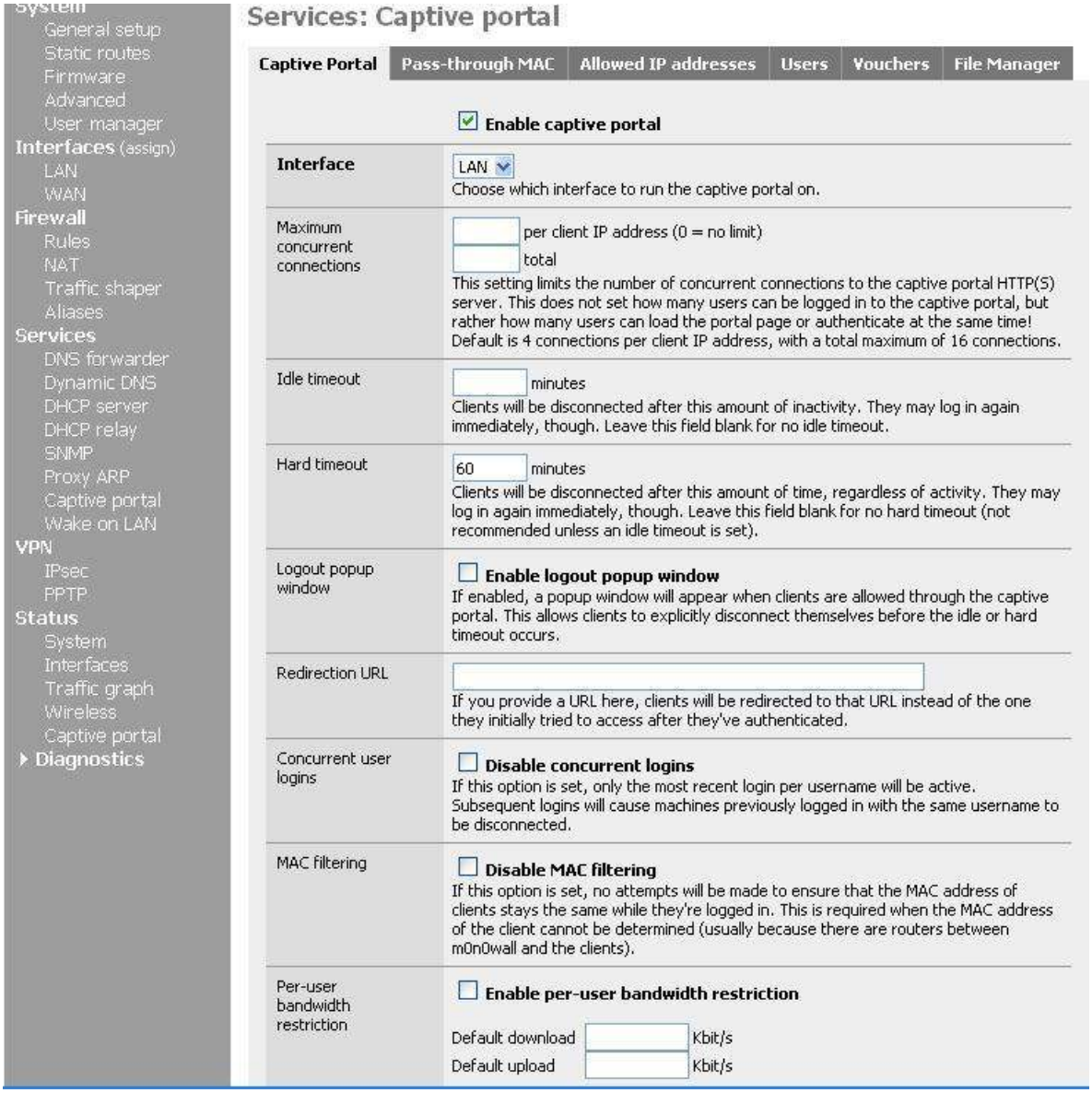
kemudian akan muncul pernyataan bahwa IP addres LAN telah diatur menggunakan alamat IP yang baru yakni 192.168.182.1/24. Sampai disini webGUI dari monowall sudah bisa diakses untuk administrasi lebih lanjut. maka akan ditampilkan permintaan untuk memasukan username beserta password sebagai proses identifikasi.

Pada saat memasuki webGUI monowall pilihlah interfaces WAN dengan type koneksi yang ingin dipergunakan(static, PPTP, DHCP, PPPoE) misalnya menggunakan tipe koneksi PPPoE (karena menggunakan akses internet ADSL), dalam PPPoE configuration masukan username dan password dari ISP yang dipergunakan, kemudian simpan proses yang dilakukan tersebut.

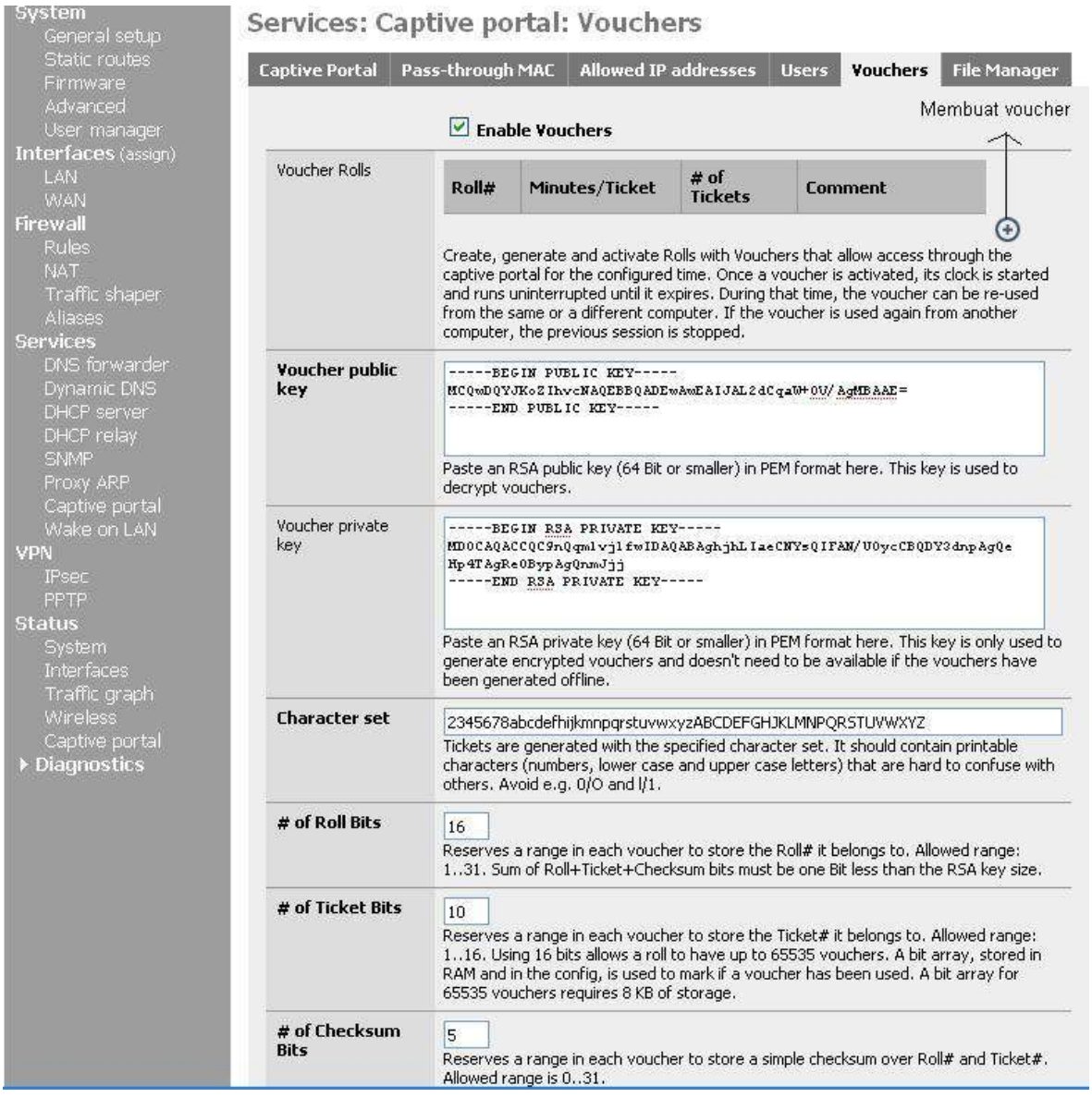
Dalam pengaturan general setup ini, admin dapat melakukan pengaturan pada host/server dengan memberikan nama domain(DNS). Pengaturan username dan password dalam mengakses webGUI, type halaman web yang dipakai (misalnya http/https)



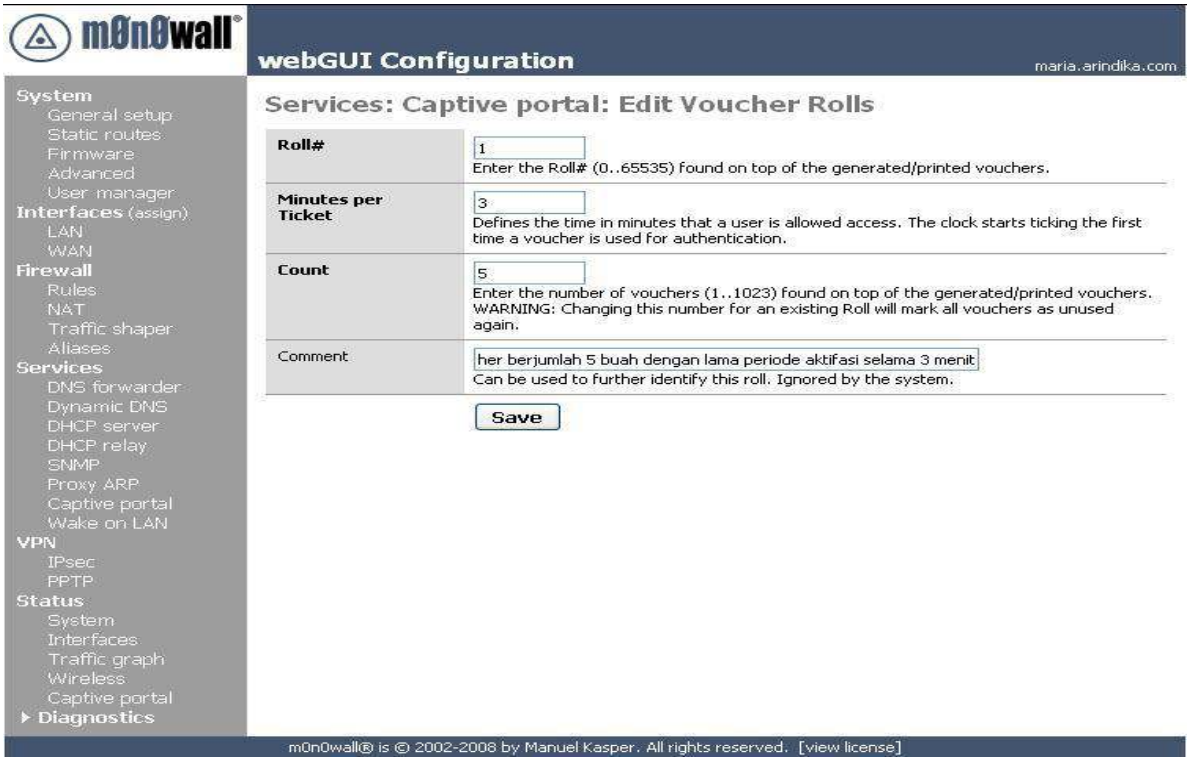
Langkah berikutnya adalah mencari bagian service, kemudian memilih captive portal. Berikan tanda checklist pada bagian enable captive portal. Pada pilihan authentication, pilih local user manager. Upload file dengan extension .html yang berisi desain portal web pada portal page contents, kemudian simpan kembali perubahan yang dilakukan.



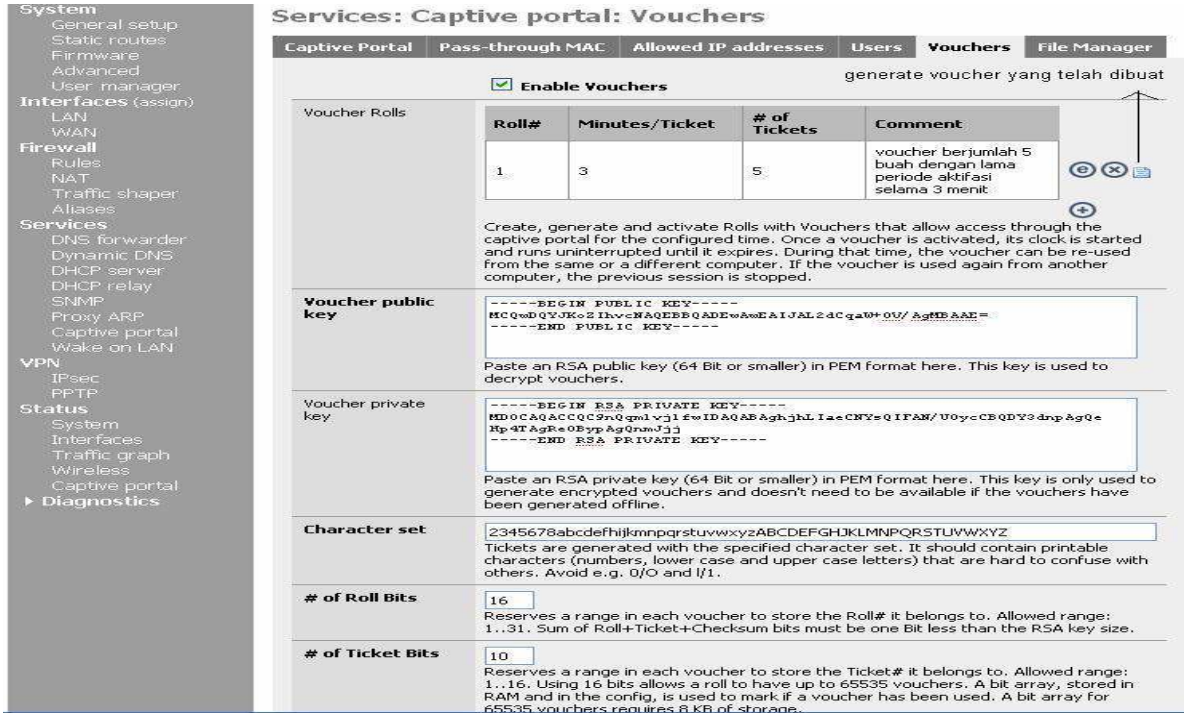
Untuk melakukan pengaturan voucher internet, pilihlah voucher, berikan tanda checklist bagian enable voucher, kemudian simpan kembali. Pilihlah tanda (+), maka akan muncul pengaturan pada proses pembuatan voucher, yakni terdiri dari jumlah voucher dan lama periode aktifasi voucher tersebut, simpan kembali perubahan yang dilakukan.



Proses pembuatan voucher terdiri dari jumlah voucher dan lama periode aktifasi voucher tersebut



Proses generate voucher(menampilkan voucher yang telah dibuat)



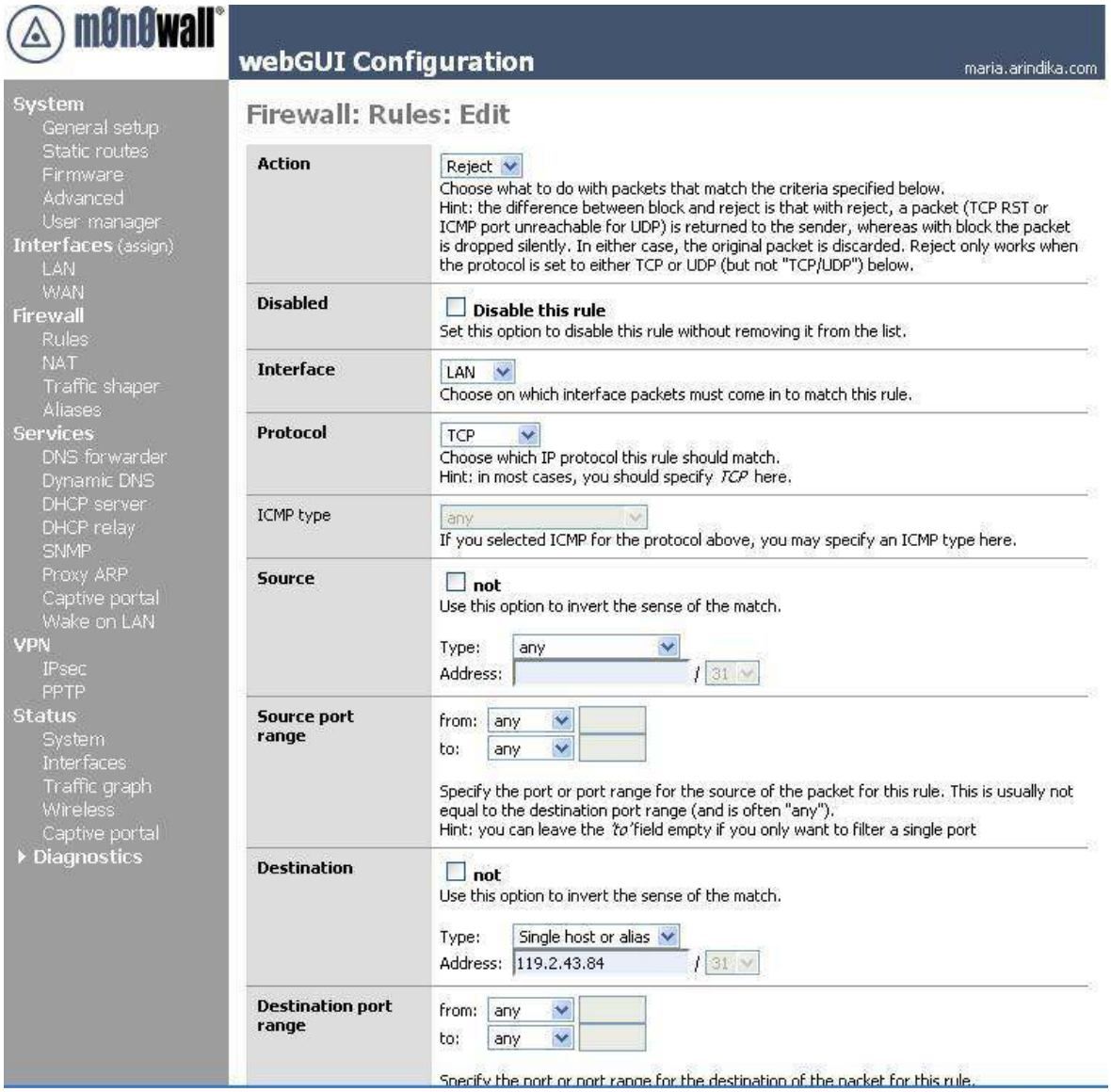
Tampilan voucher yang telah dibuat

# Voucher Tickets 1..3 for Roll 1	
# Nr of Roll Bits 16	
# Nr of Ticket Bits 10	
# Nr of Checksum Bits 5	
# magic initializer 1258256847 (32 Bits used)	
# Character Set used 2345678abcdefhijkmnpqrstuvwxyzABCDEFGHJKLMNPQRSTUVWXYZ	
#	
Pb8GEbSsccu	
Lii3EWnw4Ym	voucher
QisvyPK4tqB	

Untuk melakukan uji coba pada voucher yang telah dibuat, langkah pertama yang dilakukan adalah membuka web browser kemudian mengetikkan nama situs tertentu yang akan diakses, ketika akan mengakses situs tersebut maka permintaan pengguna akan dialihkan pada web portal yang telah dibuat sebelumnya, pada web portal ini untuk dapat melakukan akses internet pengguna harus memasukan nomor voucher pada kolom voucher yang telah disediakan.

Jika pengisian voucher benar maka permintaan pengguna pada situs tertentu akan diteruskan, srebaliknya jika vouchernya salah maka permintaan tidak akan diteruskan dan akan menampilkan gambar berikut pada webGUI pengguna.

Untuk mengatur lalu lintas paket data, dapat dilakukan dengan memberikan rules pada firewall, rules sendiri terdiri dari aceppt, deny dan reject. Contoh pengaturan rules pada monowall adalah sebagai berikut :

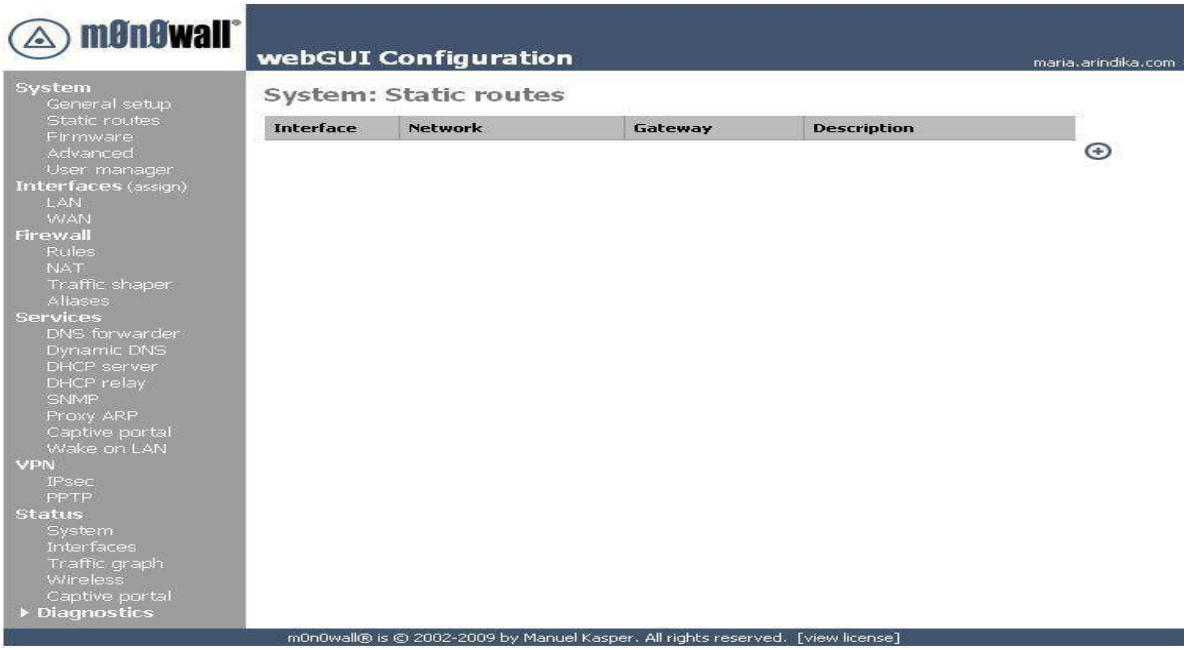


Selain itu terdapat fitur-fitur lain pada monowall yang dapat dipergunakan atau membantu proses kinerja dari suatu firewall diantaranya adalah sebagai berikut :

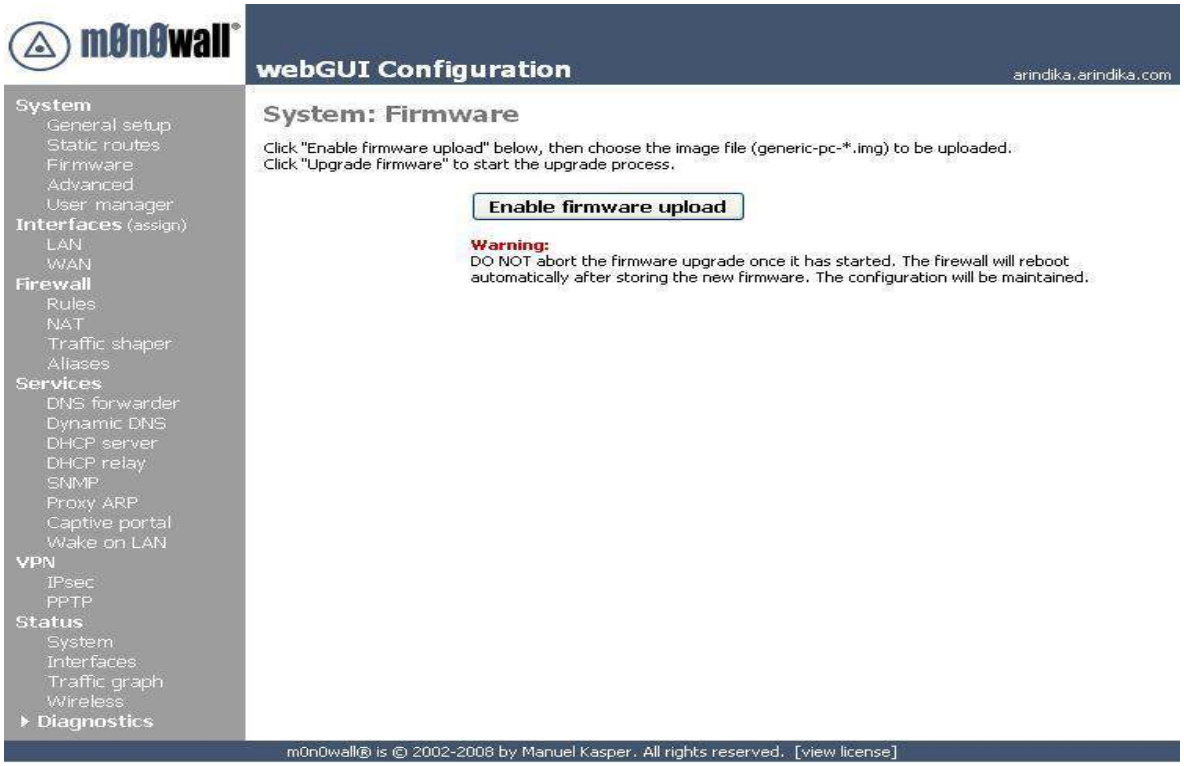
System :

- General setup(sudah dibahas sebelumnya)
- Static routes
- Firmware
- Advanced
- User manager

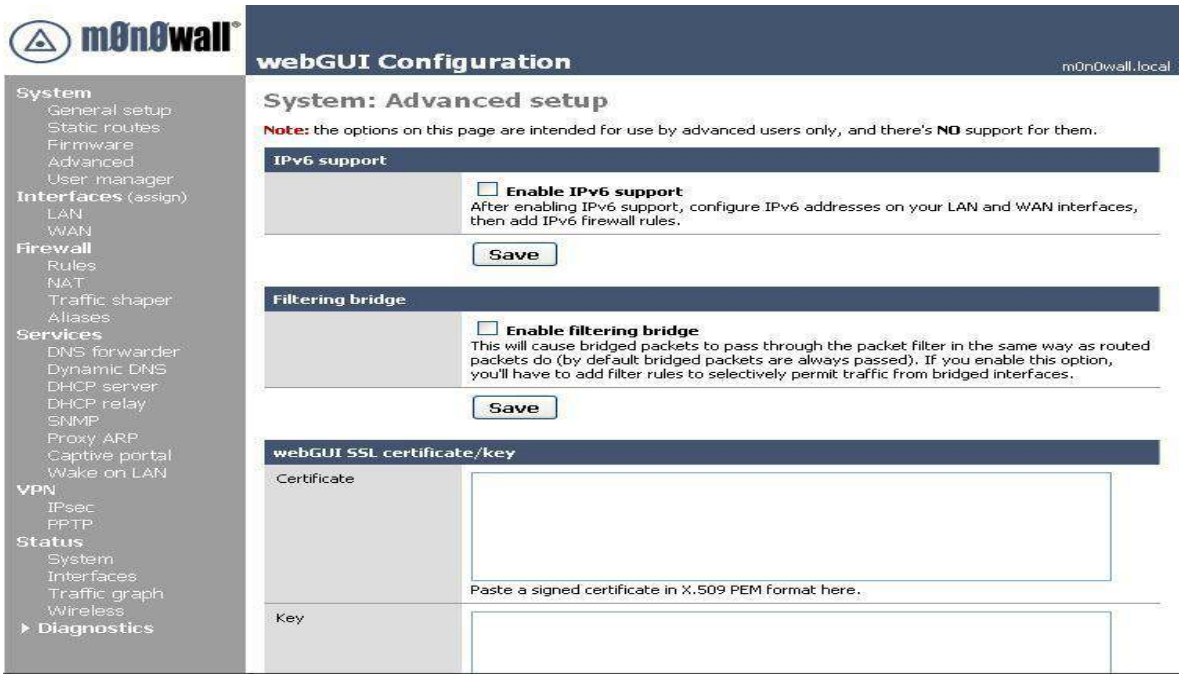
Pengaturan static routes pada monowall



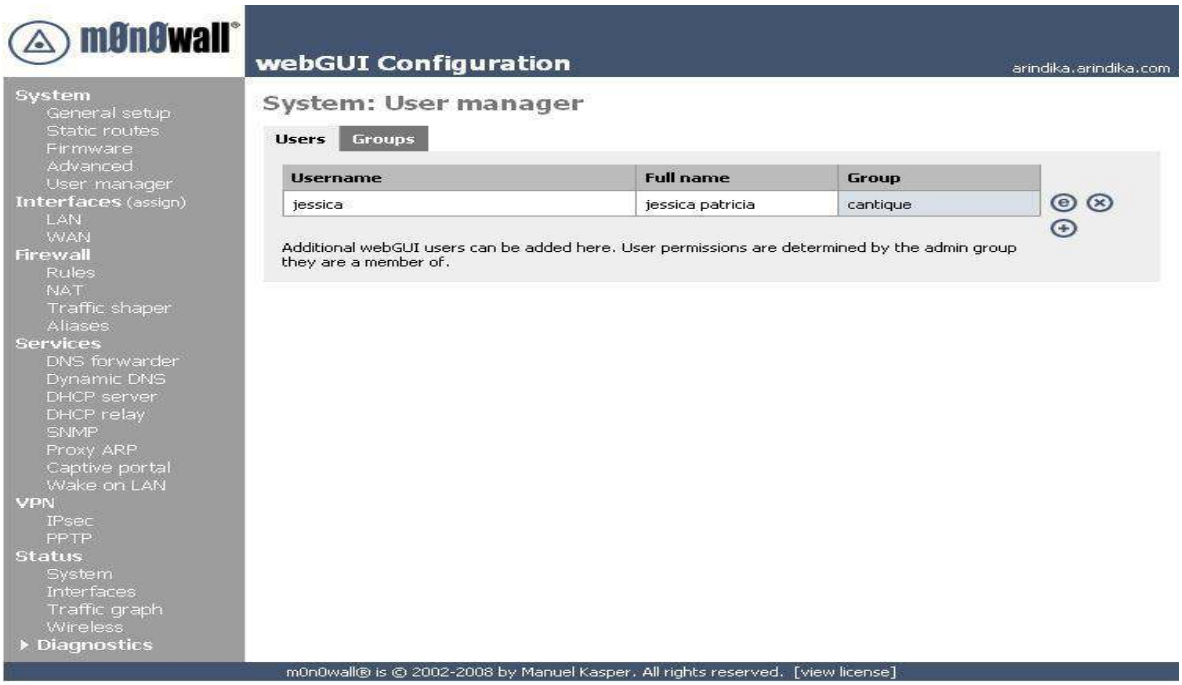
Pengaturan firmware pada monowall yang bertujuan untuk memperbaharui image binary terbaru



Pengaturan advanced setup yang dapat dipergunakan bila hendak menambahkan pengaturan tertentu pada monowall.



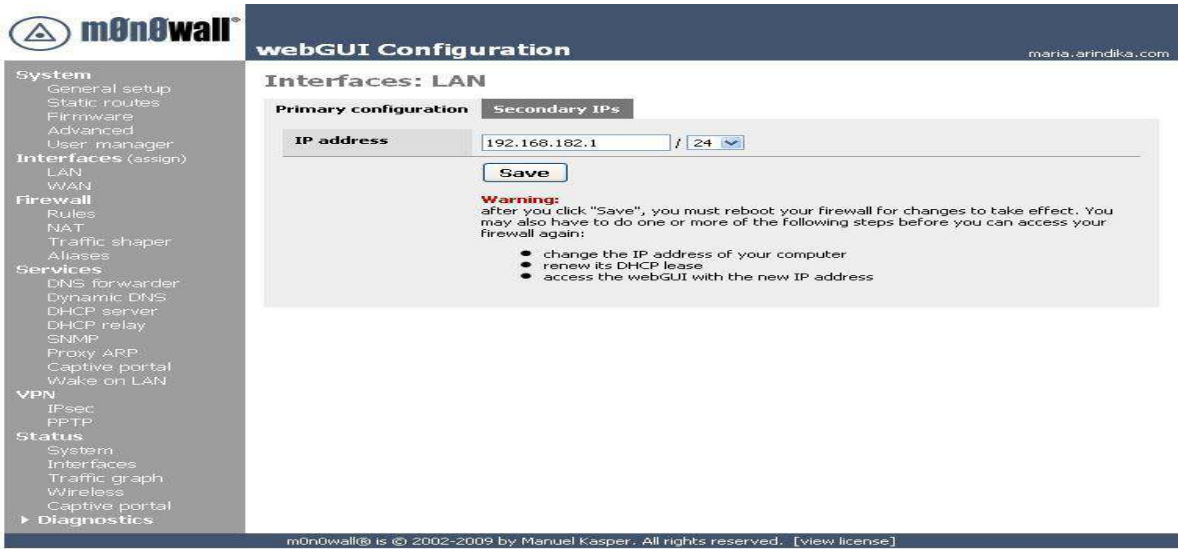
Pengaturan user manager yang terdiri dari nama admin yang dapat melakukan manage pada webGUI monowall, di sini dapat dilakukan pembagian pada admin mengenai halaman webGUI mana saja yang dapat diakses..



Interfaces (assign) :

- LAN
- WAN(Pengaturan interface WAN telah dibahas sebelumnya)

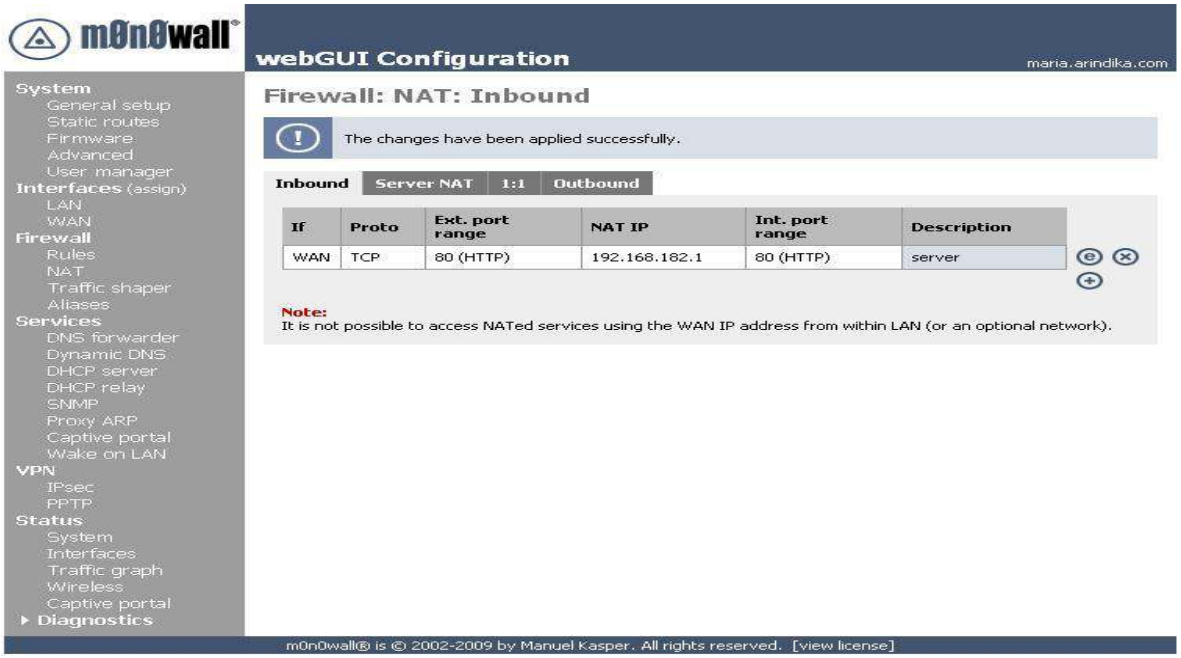
Pengaturan interface LAN



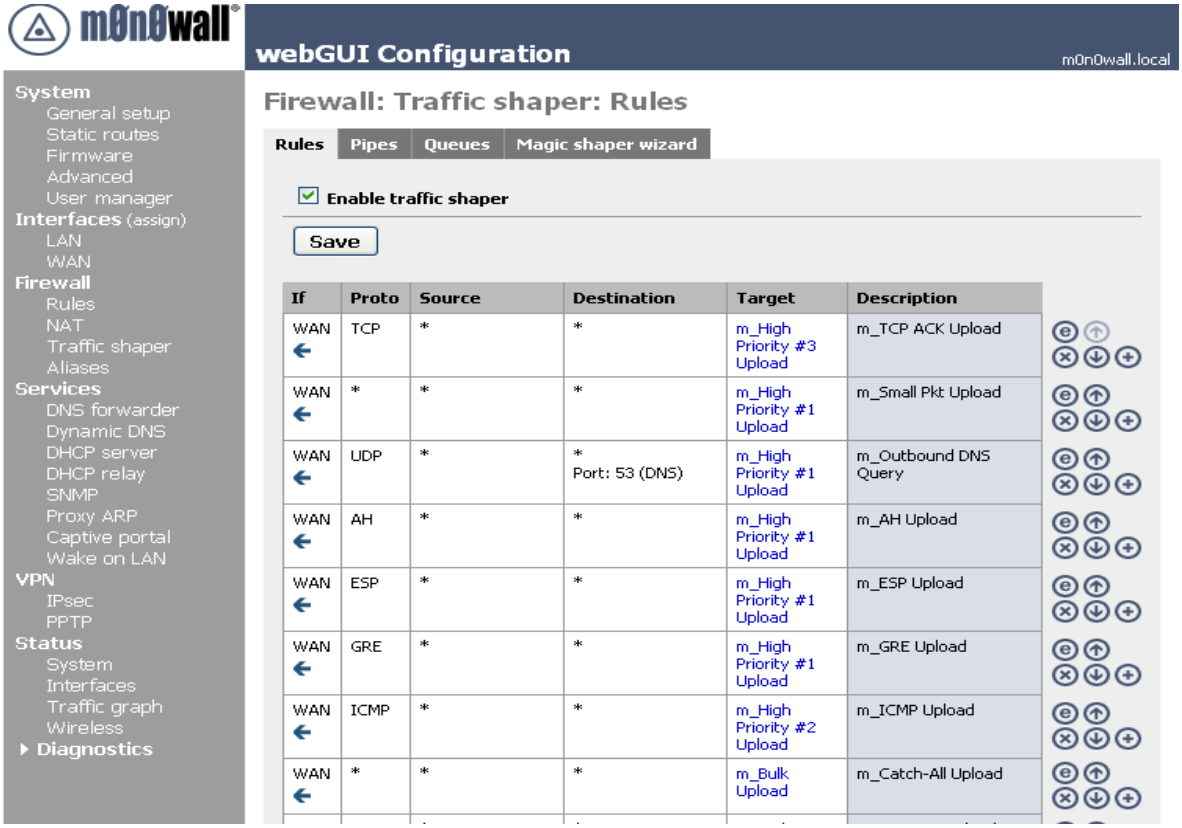
Firewall :

- Rules(Pengaturan rules telah dibahas sebelumnya)
- NAT
- Traffic Shaper
- Aliases

Pengaturan NAT



Pengaturan traffic shaper



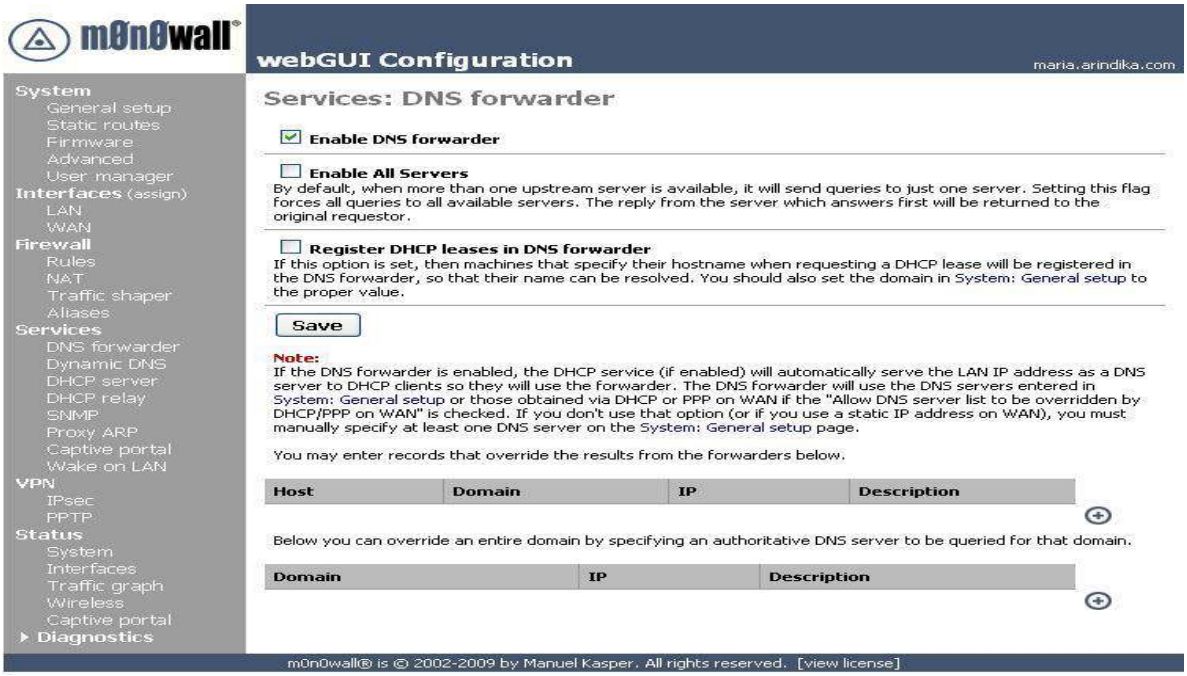
Pengaturan aliases

Services :

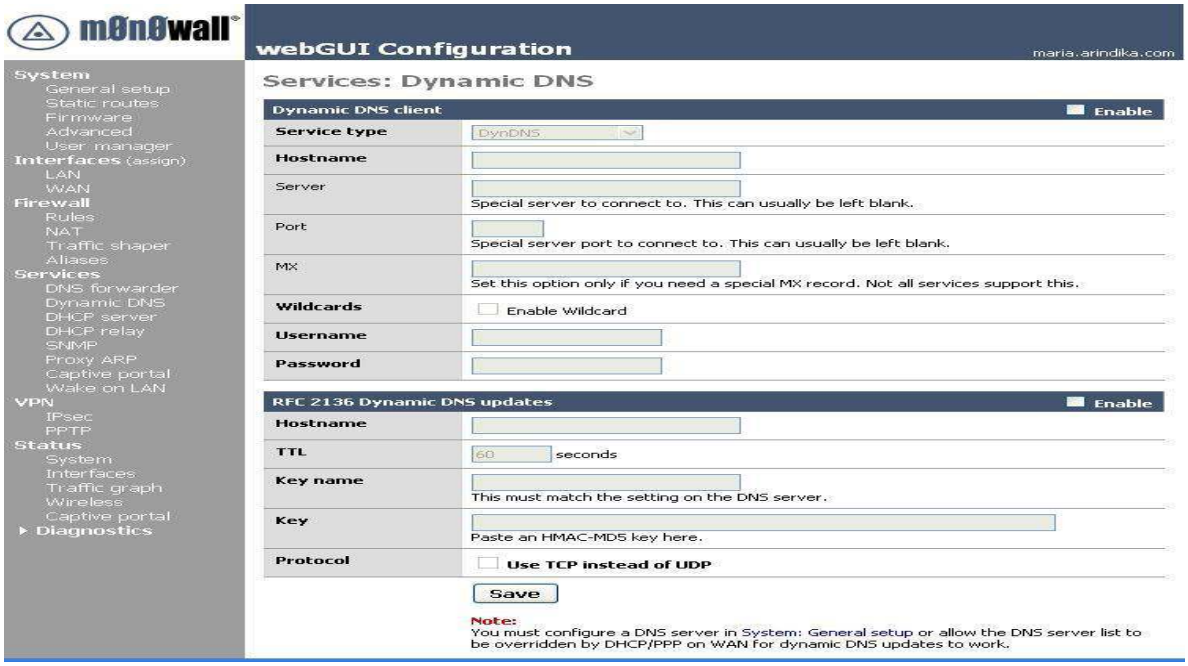
- DNS Forwader
- Dynamic DNS

- DHCP Server
- DHCP relay
- SNMP
- Proxy ARP
- Captive Portal(Telah dibahas sebelumnya)
- Wake on LAN

Pengaturan DNS Forwarder

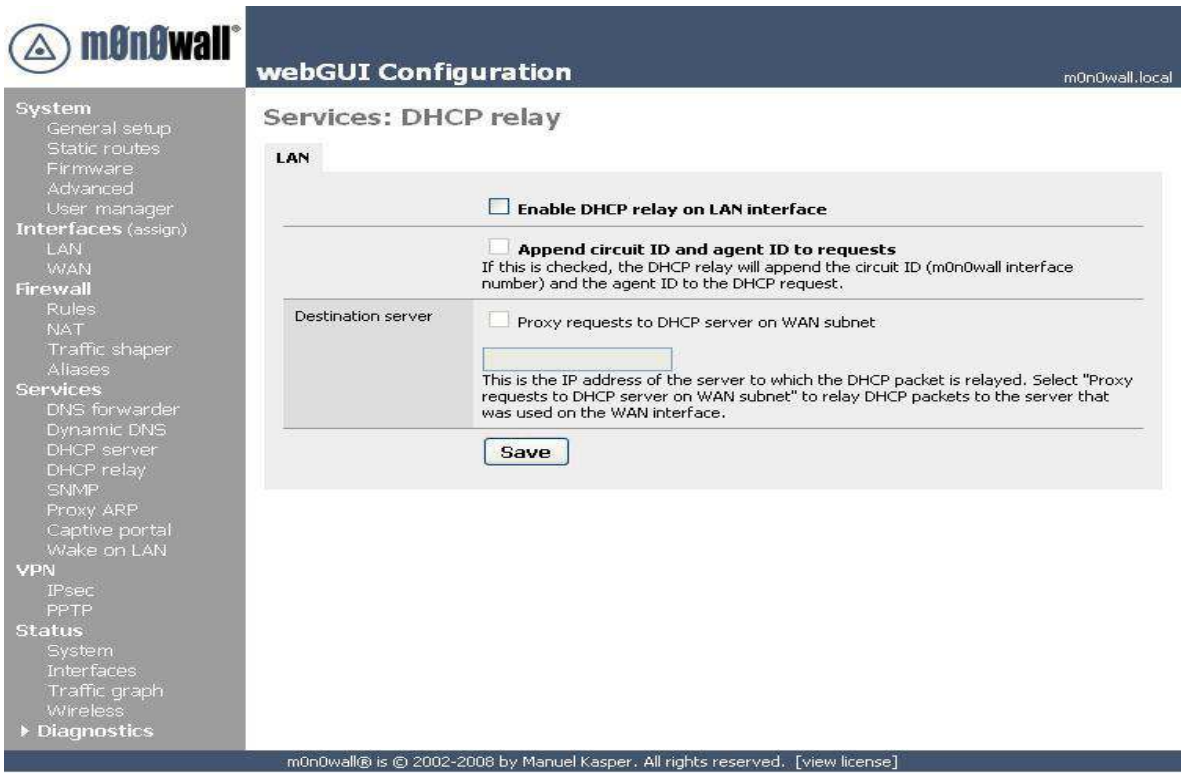


Pengaturan Dynamic DNS

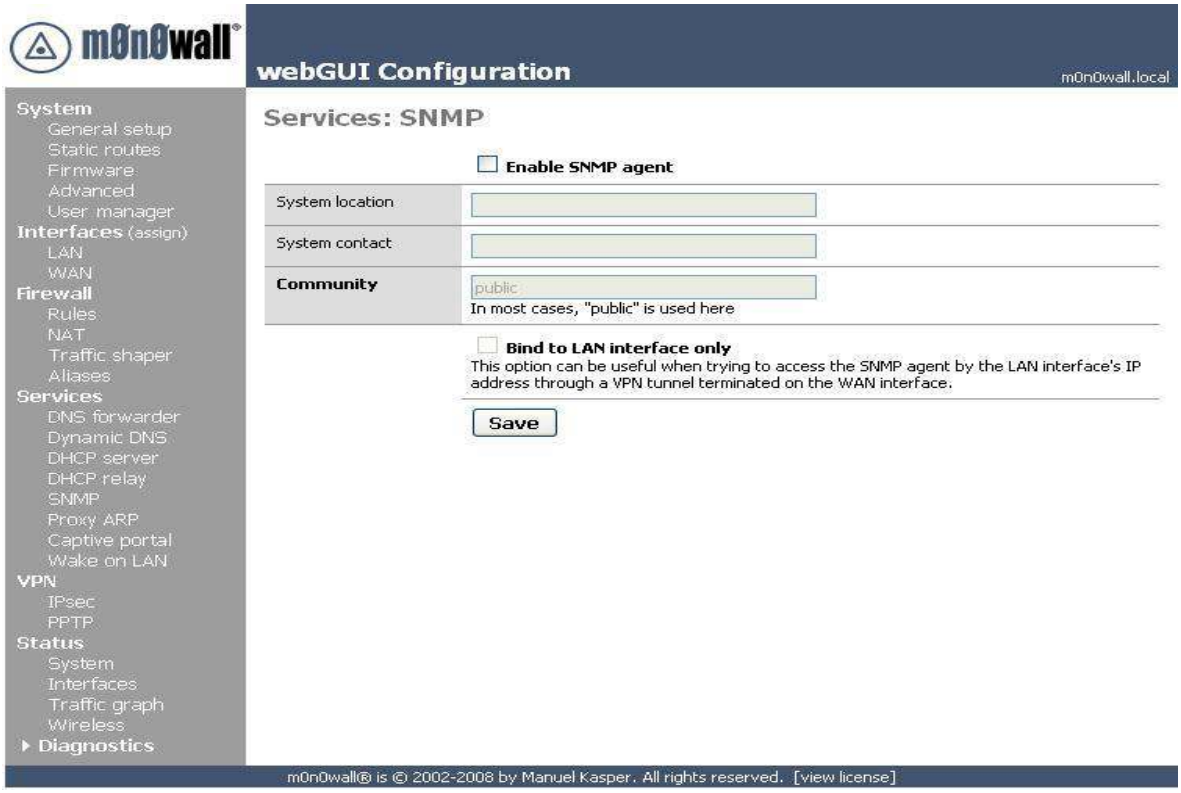


Pengaturan DHCP server

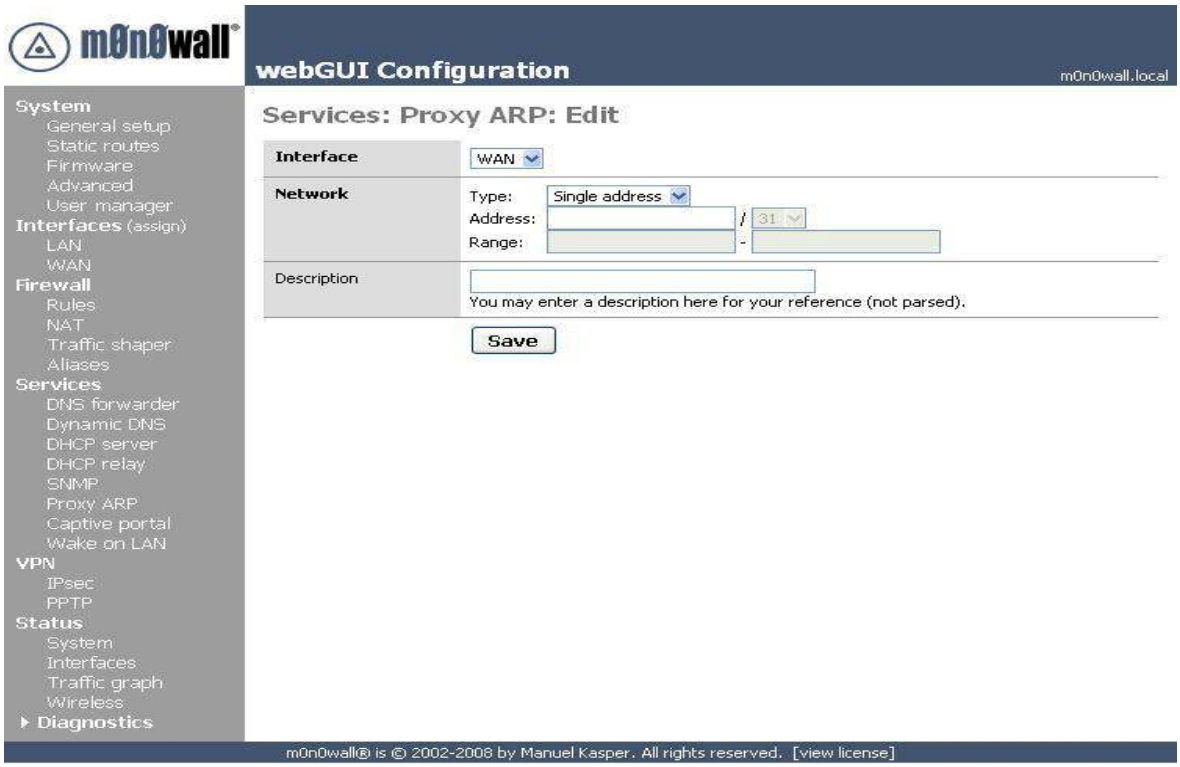
Pengaturan DHCP relay



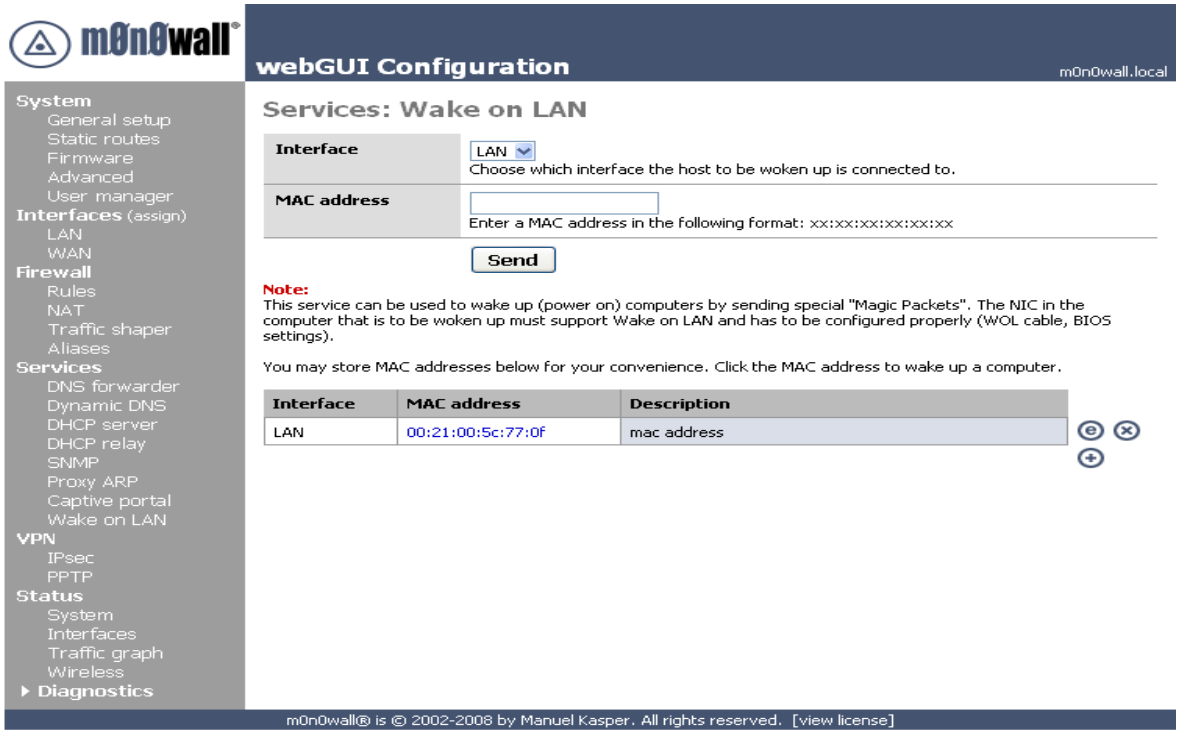
Pengaturan SNMP



Pengaturan proxy ARP

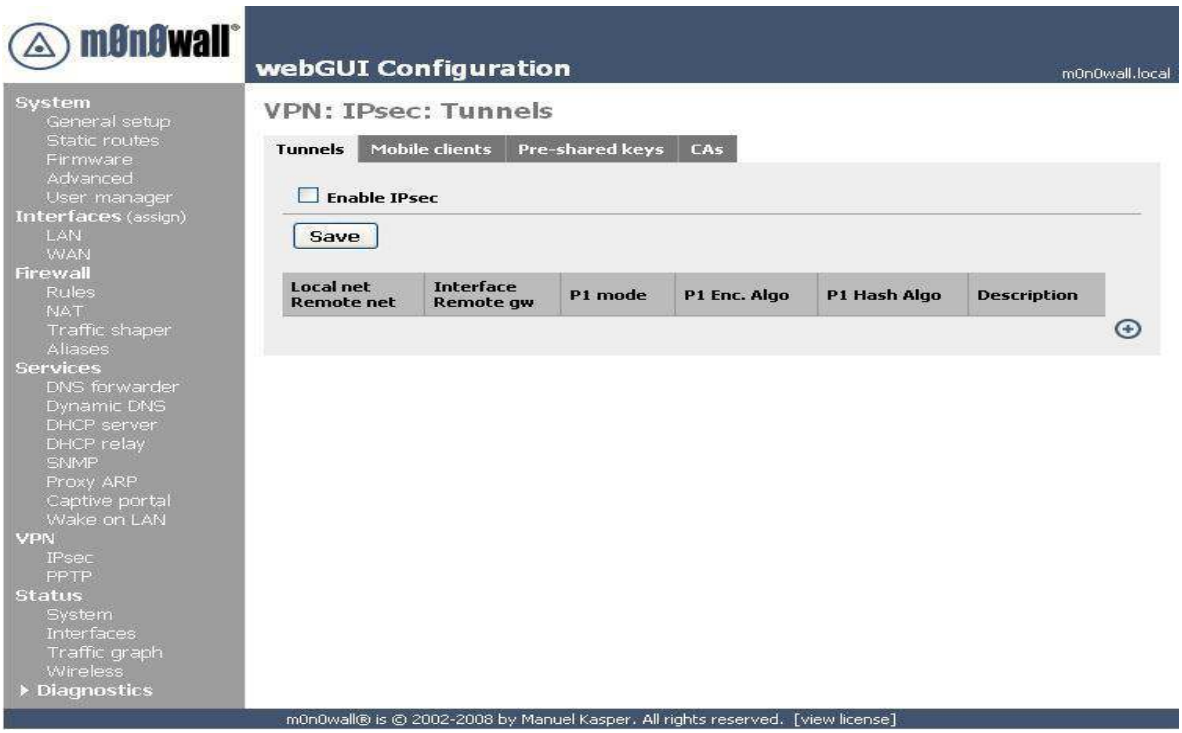


Pengaturan Wake on LAN

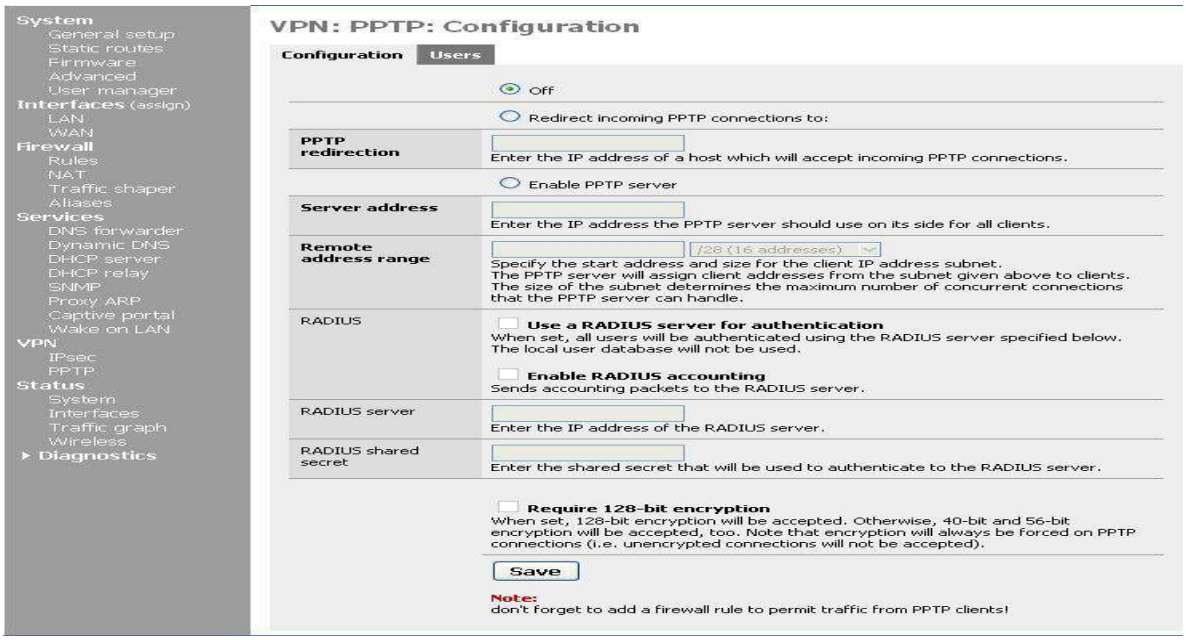


VPN :
- IPsec
- PPTP

Pengaturan IPsec



Pengaturan PPTP

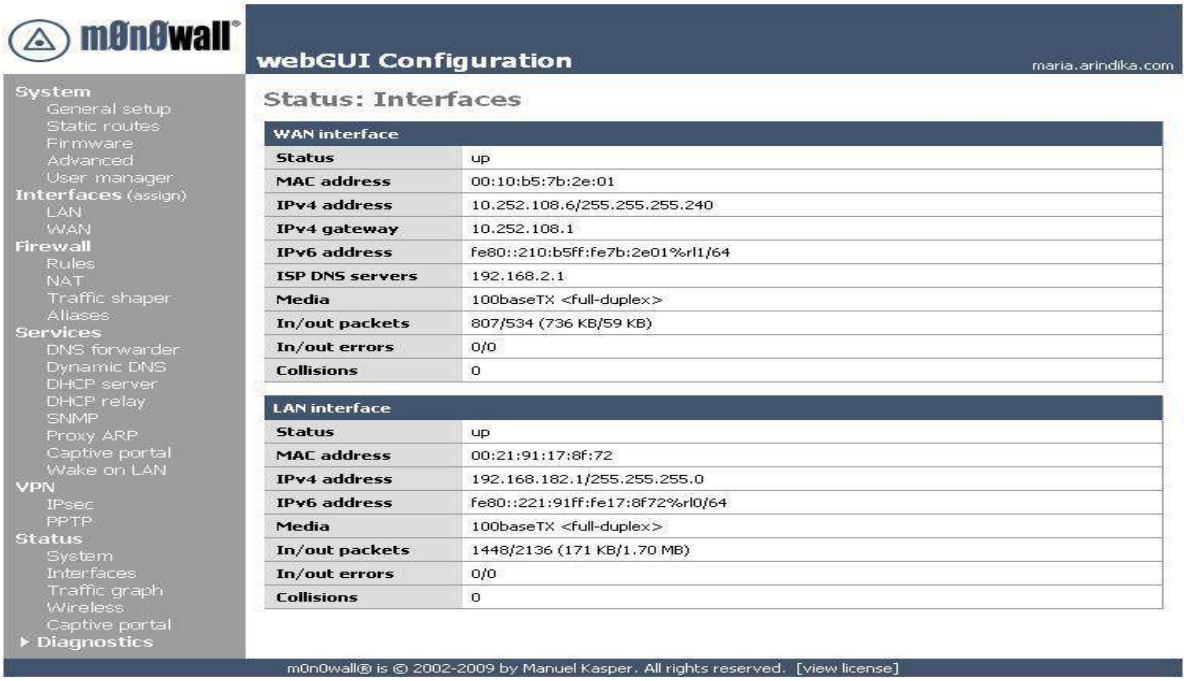


Status :

- System (Tampilan menu utama)
- Interfaces
- Traffic graph
- wireless

Tampilan system

Mengetahui status interfaces



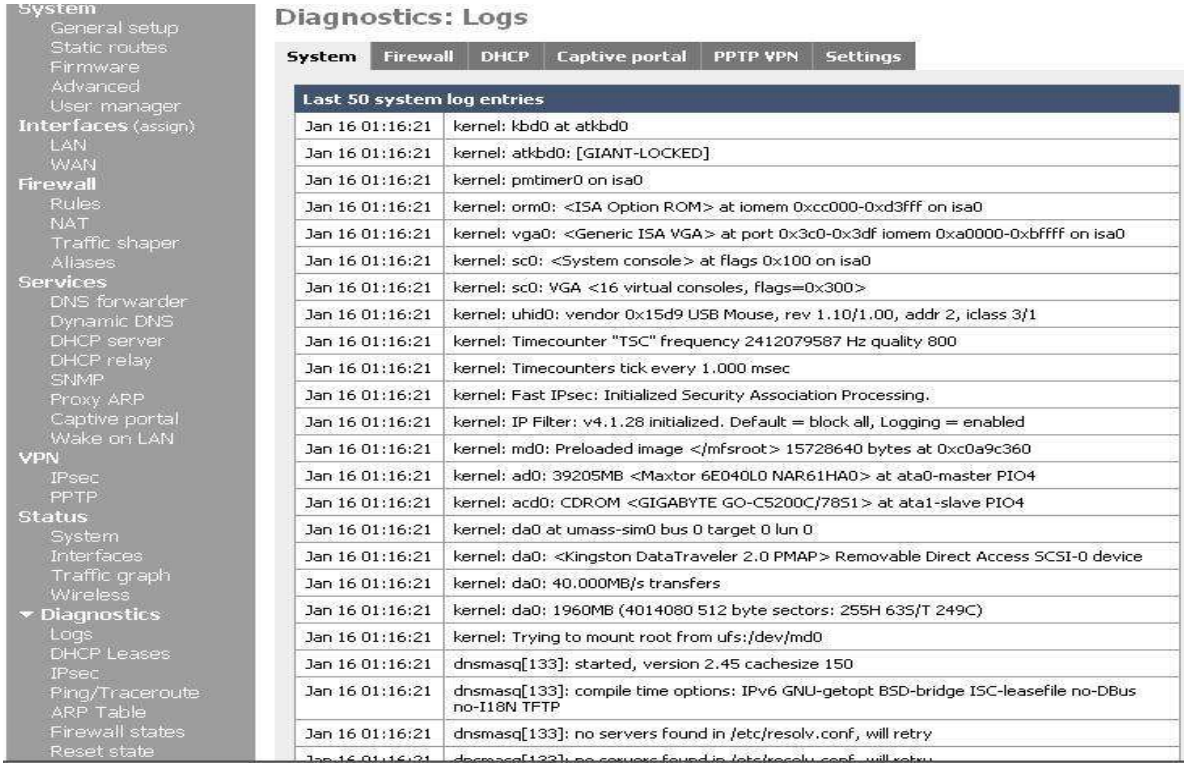
Mengetahui aktifitas download

Status wireless

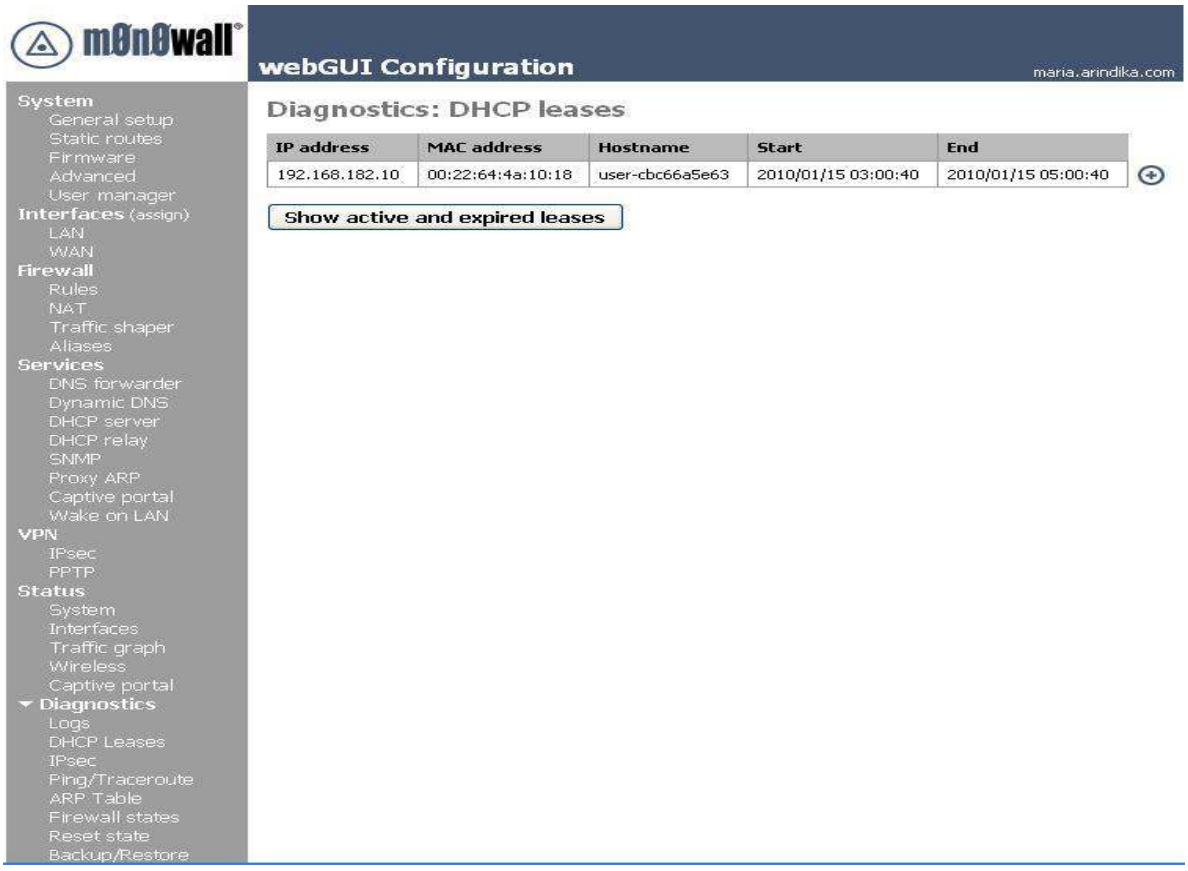
Diagnostics :

- Logs
- DHCP Leases
- IPsec
- Ping/traceroute
- ARP Table
- Firewall states
- Reset state
- Backup/restore
- Factory defaults
- Reboot system

Status Logs(mencatat segala aktifitas yang dilakukan)

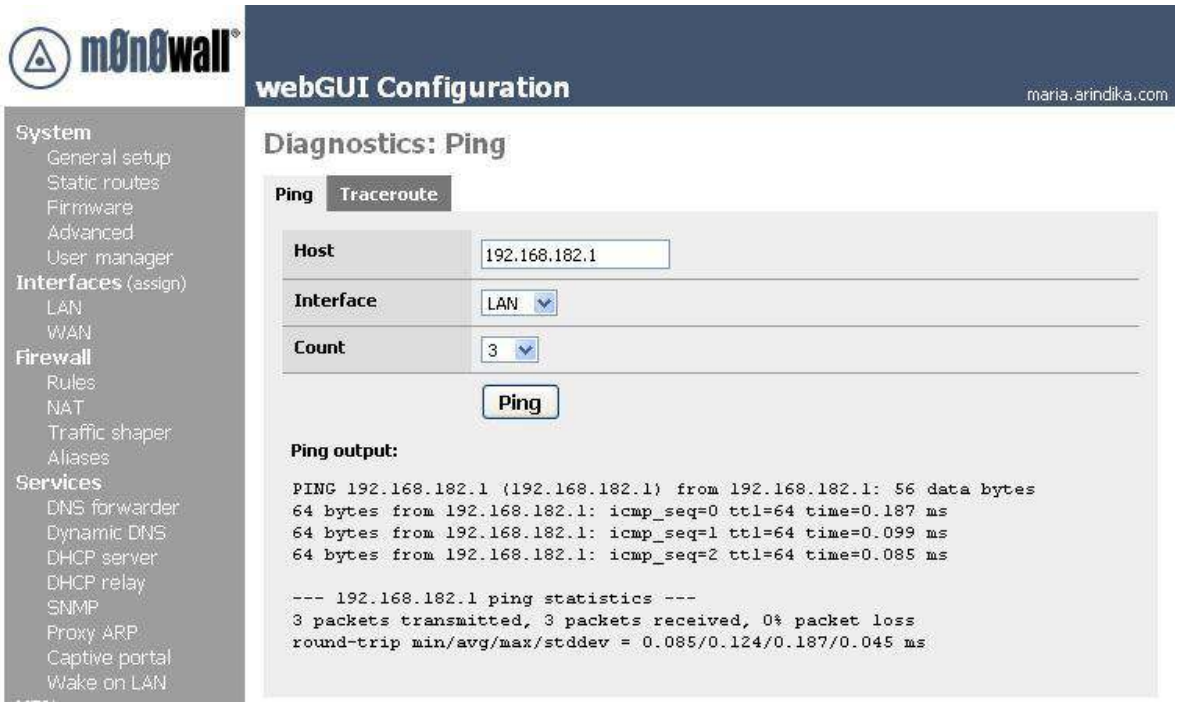


Penyewaan alamat IP

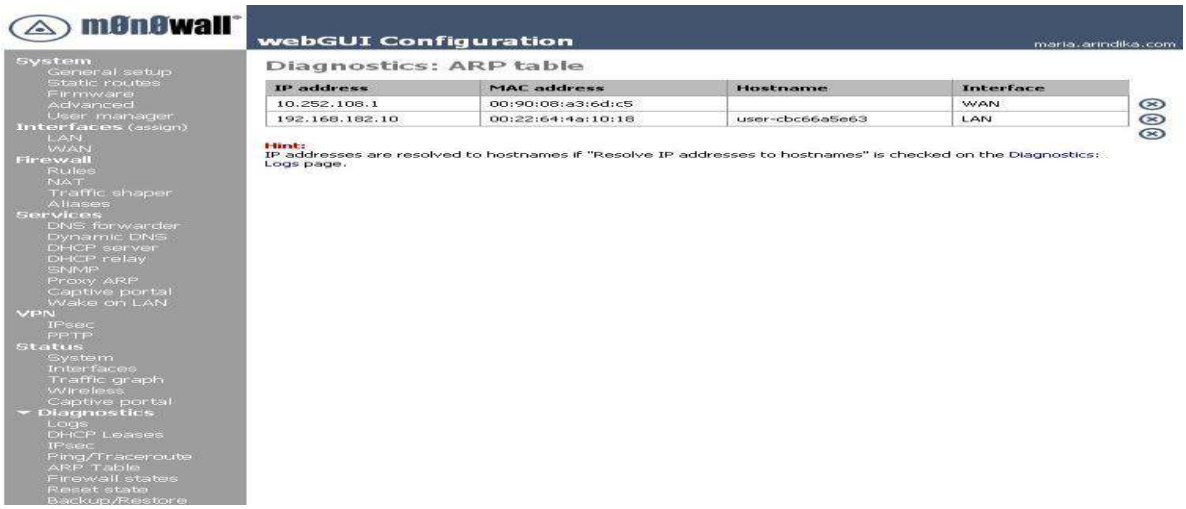


IPsec

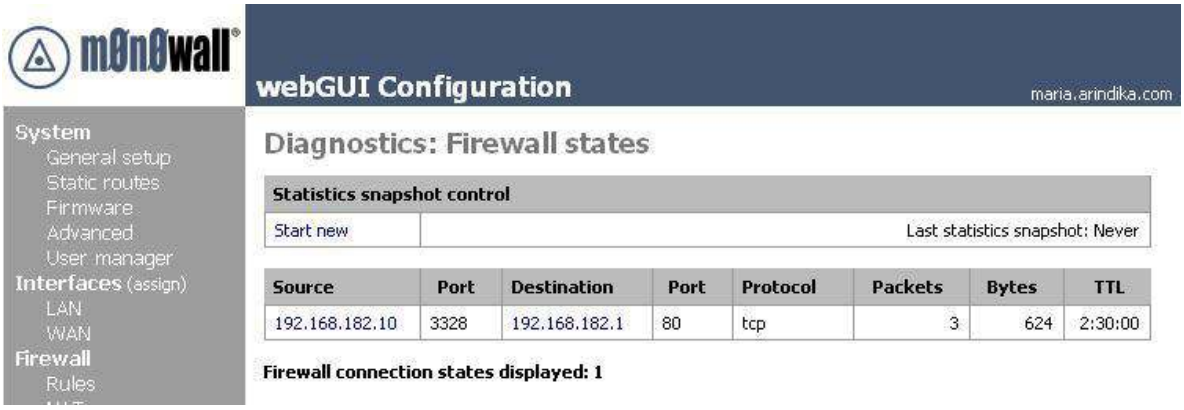
Ping IP address



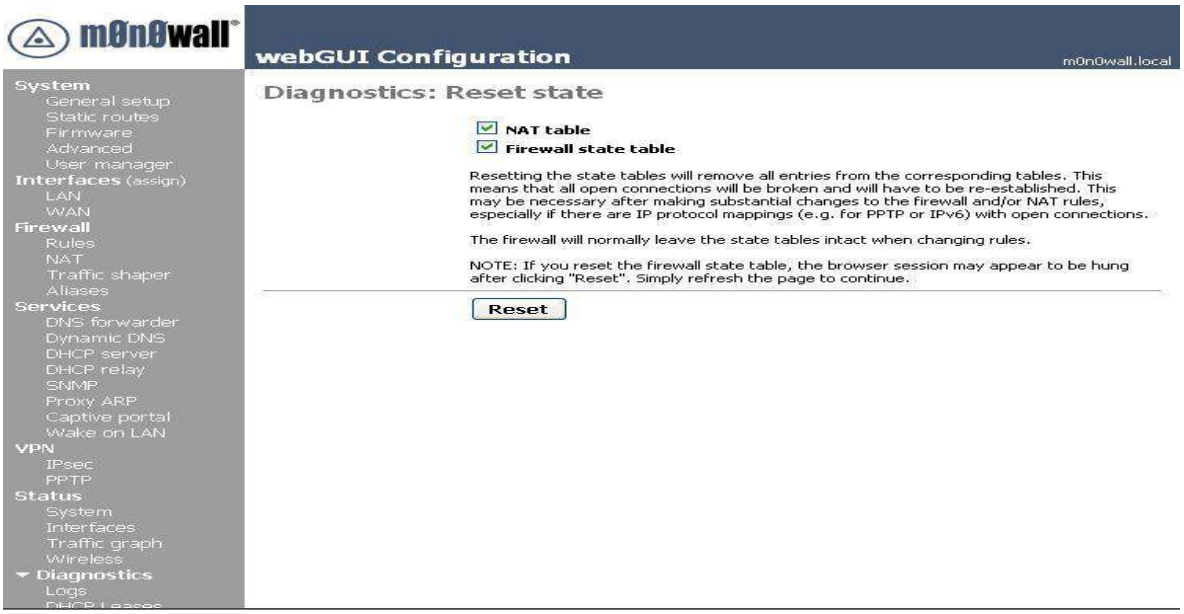
ARP Table



Firewall states

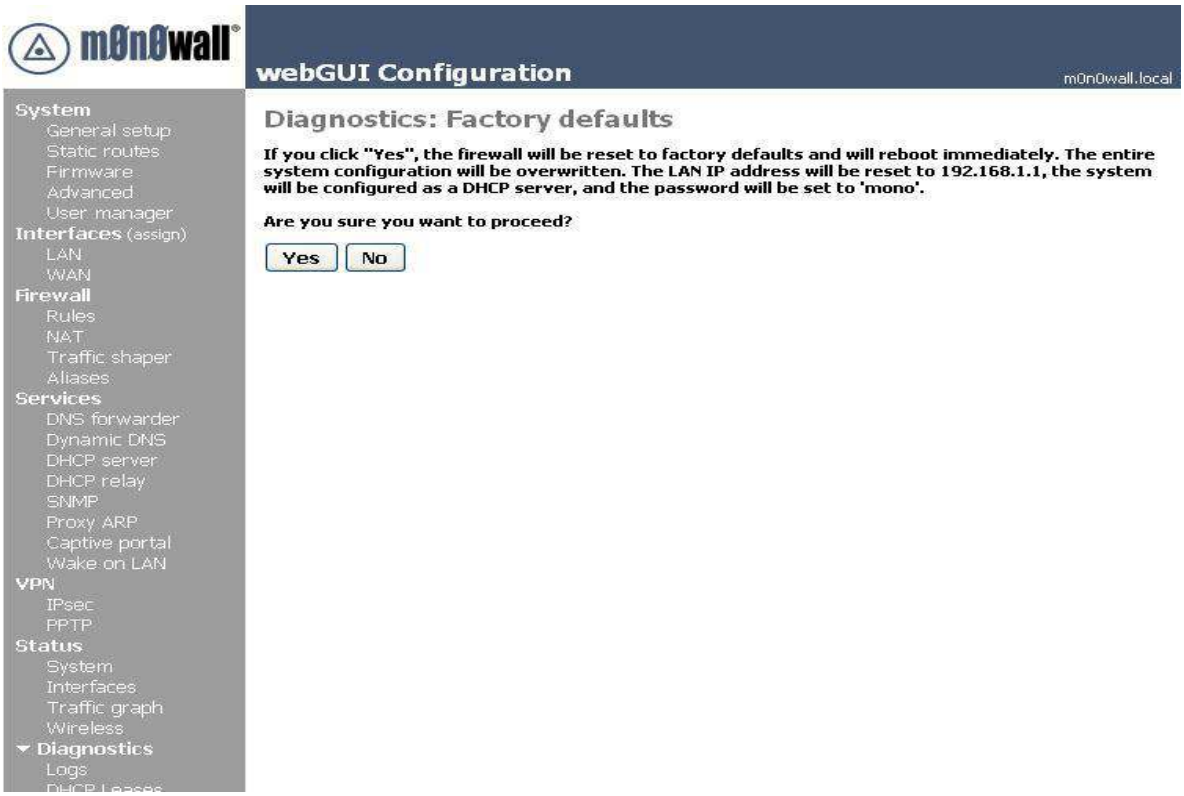


Reset states

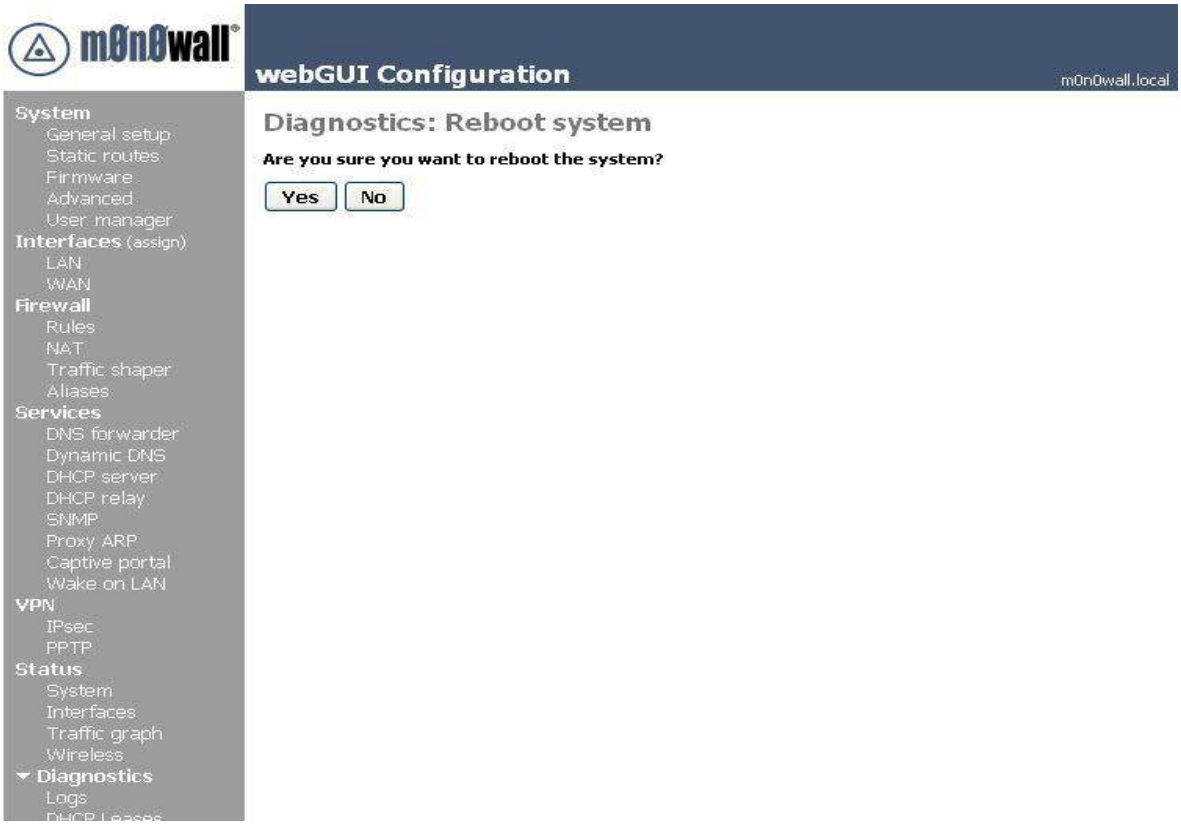


Backup and restore

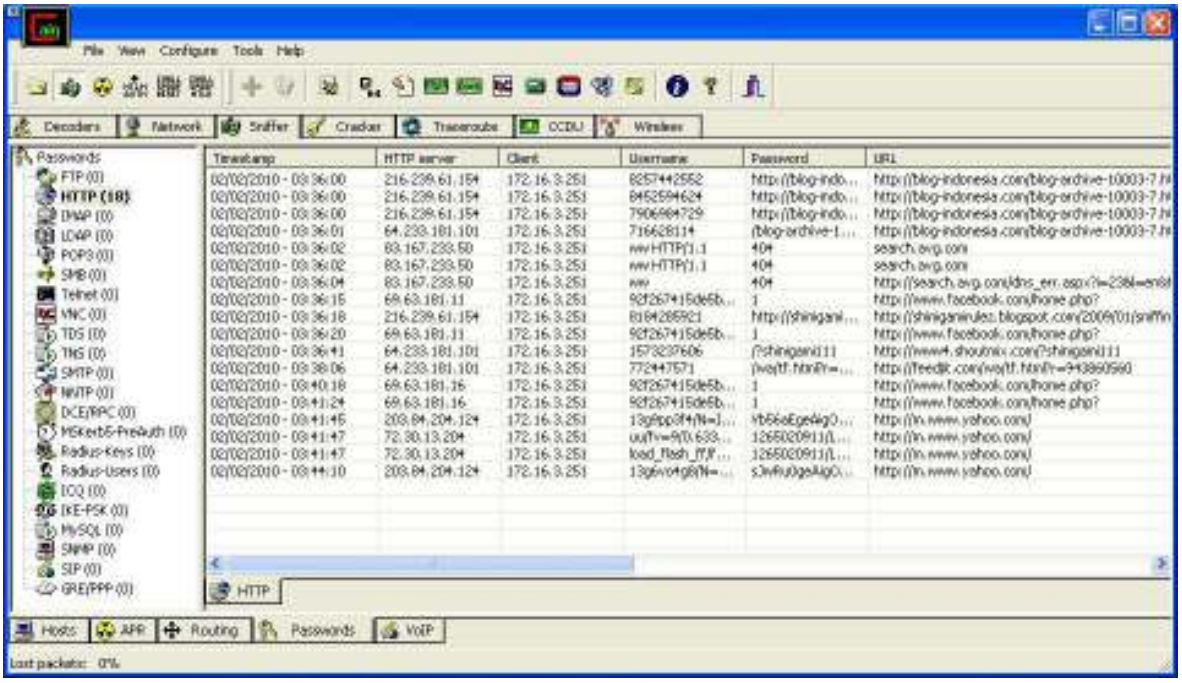
Factory defaults



Reboot system

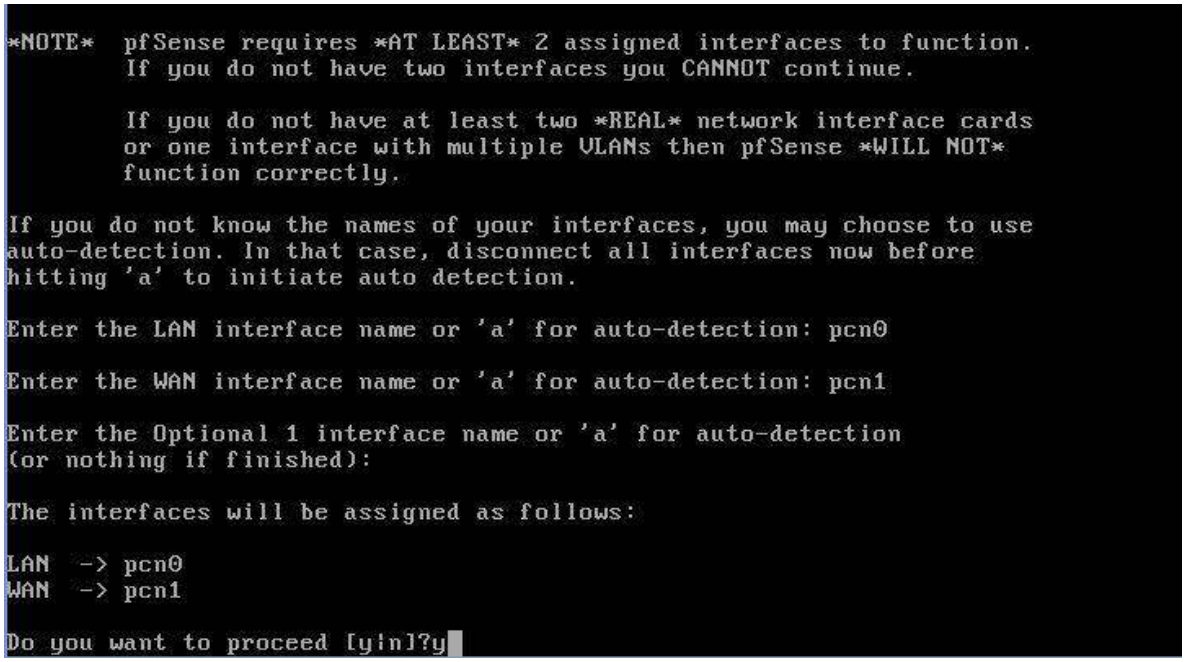


Pengujian aksi sniffing menggunakan software cain & able menangkap situs tertentu yang diakses pengguna, tetapi tidak dapat menangkap password pengguna secara jelas.



2.1 Pfsense

Untuk proses konfigurasi dilakukan melalui proses instalasi pada hardisk komputer, pfsense seperti halnya monowall memilki bentuk konfigurasi yang hampir sama, hal ini dikarenakan pfsense merupakan bentuk pengembangan dari monowall. Langkah pertama yang akan dilakukan untuk mengkonfigurasi pfsense adalah melakukan pengaturan pada interfaces (NIC) dan IP address (pada tahap ini proses pengaturannya sama dengan monowall seperti yang telah dibahas sebelumnya), selanjutnya akan dilakukan akses pada webGUI pfsense beserta pengaturan modem ADSL speedy menjadi bridging.



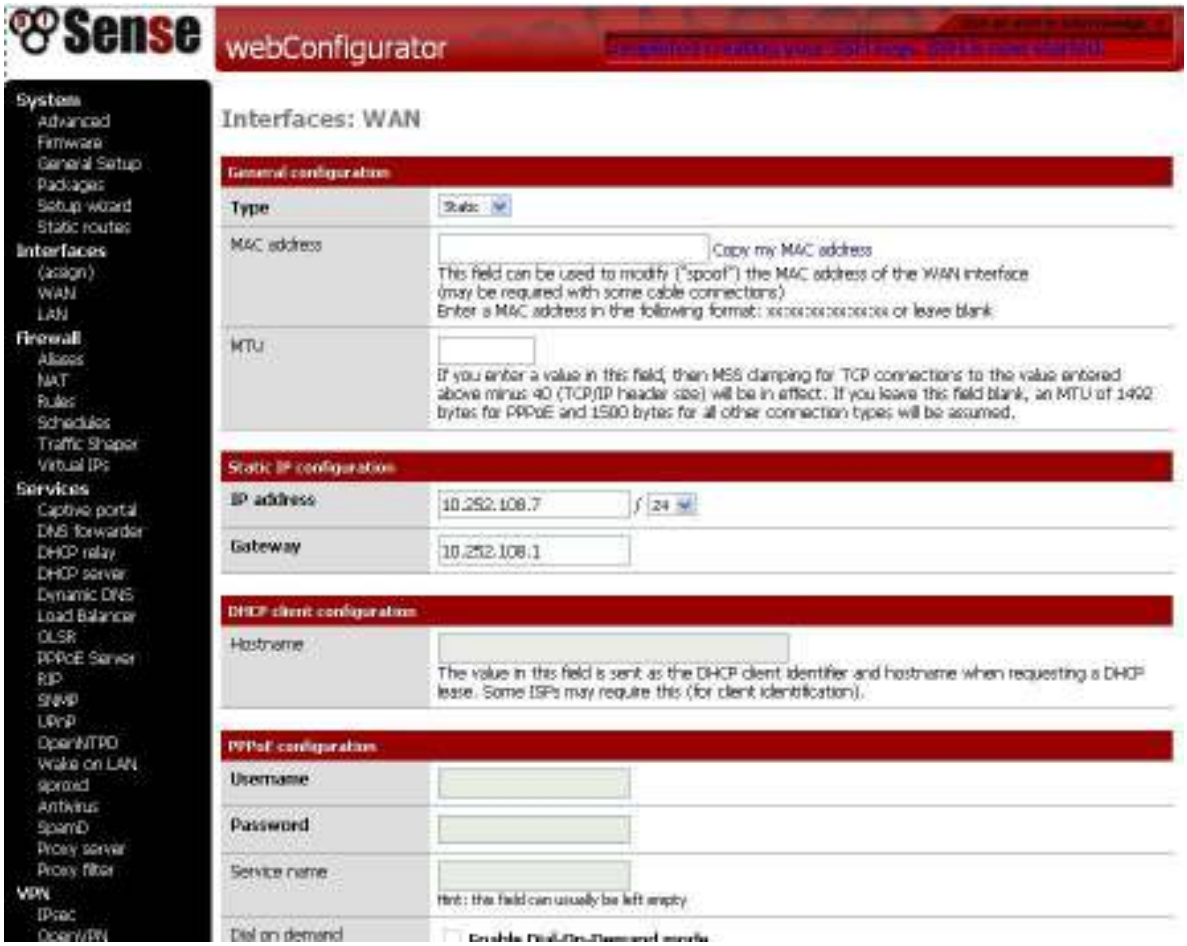
```
 LAN*                    ->   pcn0    ->      192.168.1.1
 WAN*                    ->   pcn1    ->      0.0.0.0(DHCP)

 pfSense console setup
*************************
 0)  Logout (SSH only)
 1)  Assign Interfaces
 2)  Set LAN IP address
 3)  Reset webConfigurator password
 4)  Reset to factory defaults
 5)  Reboot system
 6)  Halt system
 7)  Ping host
 8)  Shell
 9)  PFtop
10)  Filter Logs
11)  Restart webConfigurator
12)  pfSense PHP shell
13)  Upgrade from console
14)  Enable Secure Shell (sshd)
99)  Install pfSense to a hard drive/memory drive, etc.


Enter an option: 2
```

```
 8)  Shell
 9)  PFtop
10)  Filter Logs
11)  Restart webConfigurator
12)  pfSense PHP shell
13)  Upgrade from console
14)  Enable Secure Shell (sshd)
99)  Install pfSense to a hard drive/memory drive, etc.


Enter an option: 2


Enter the new LAN IP address: 192.168.1.5

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN subnet bit count: 24

Do you want to enable the DHCP server on LAN [y|n]?  y
Enter the start address of the client address range: 192.168.1.6
Enter the end address of the client address range: 192.168.1.20
```

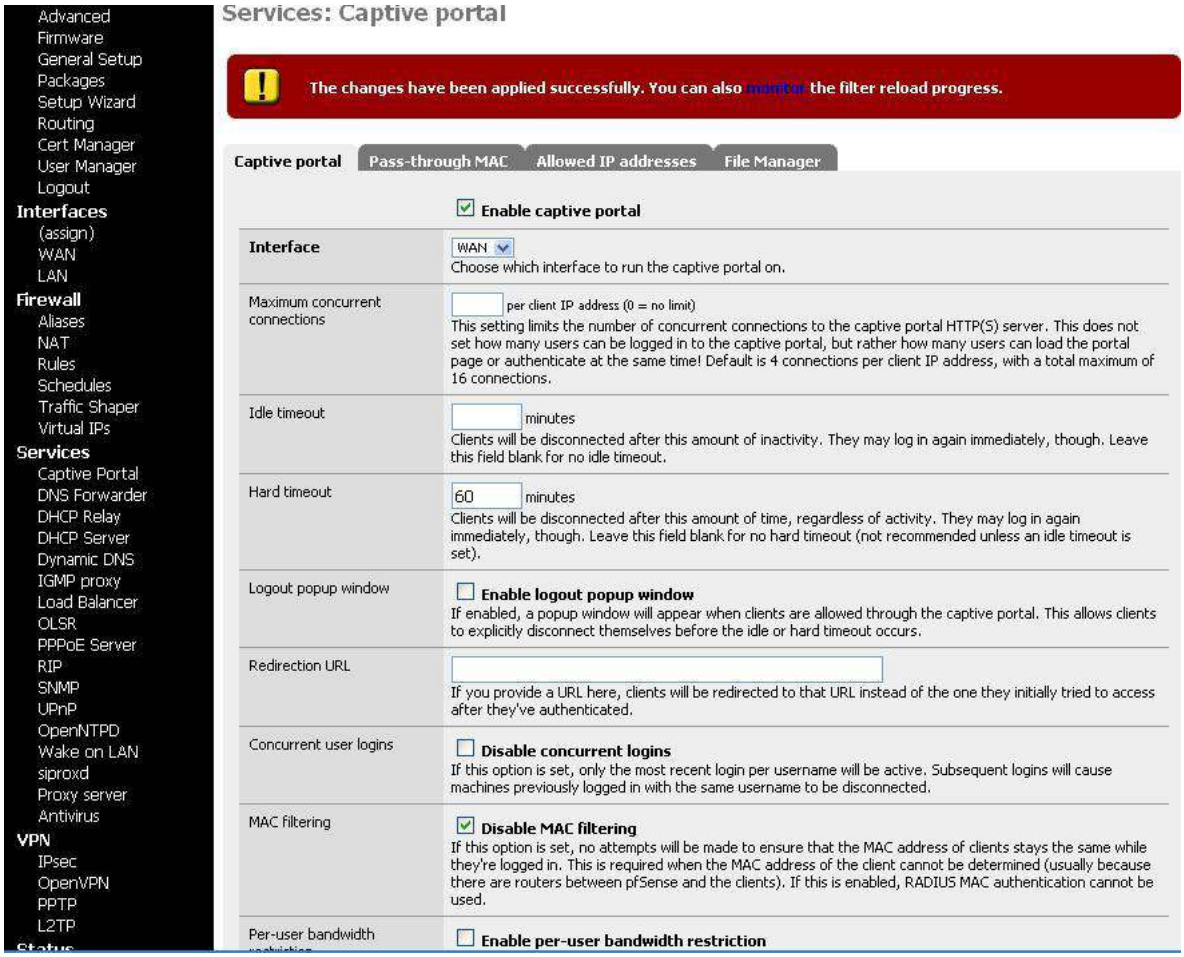
```
Enter an option: 2


Enter the new LAN IP address: 192.168.1.5

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN subnet bit count: 24

Do you want to enable the DHCP server on LAN [y|n]?  y
Enter the start address of the client address range: 192.168.1.6
Enter the end address of the client address range: 192.168.1.20

The LAN IP address has been set to 192.168.1.5/24.
You can now access the webGUI by opening the following URL
in your web browser:

http://192.168.1.5/

Press ENTER to continue.
```

Pada gambar-gambar diatas telah diperlihatkan proses konfigurasi interfaces LAN/WAN serta konfigurasi pada IP address. Pada saat melakukan akses pada http ://192.168.1.1/24 di web browser di sisi client, maka akan ditampilkan permintaan untuk memasukan username beserta password sebagai proses identifikasi.

Langkah selanjutnya adalah memilih interfaces WAN dengan tipe koneksi yang dipergunakan (PPPoE, PPTP, static, DHCP), bila mempergunakan tipe koneksi PPPoE, maka dalam PPPoE configuration akan dimasukkan username dan password dari ISP yang dipergunakan kemudian simpan perubahan yang dilakukan tersebut(penjelasan dapat dilihat pada gambar di bawah ini).



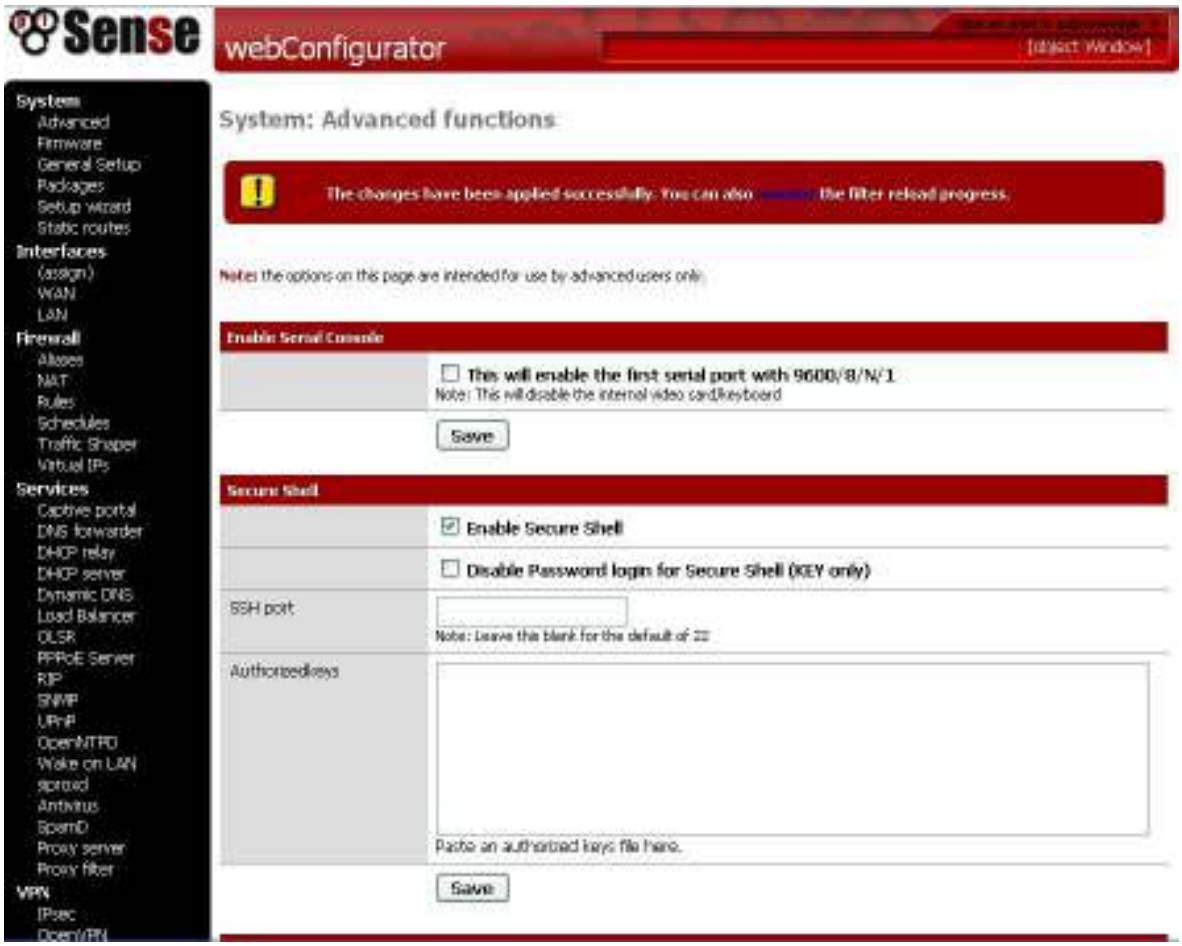
Untuk pengaturan captive portal pada bagian service pilihlah captive portal, beri tanda checklist pada bagian enable captive portal, disable MAC filtering, local user manager, kemudian upload portal page yang telah dibuat sebelumnya, simpan perubahan yang telah dilakukan.



System :

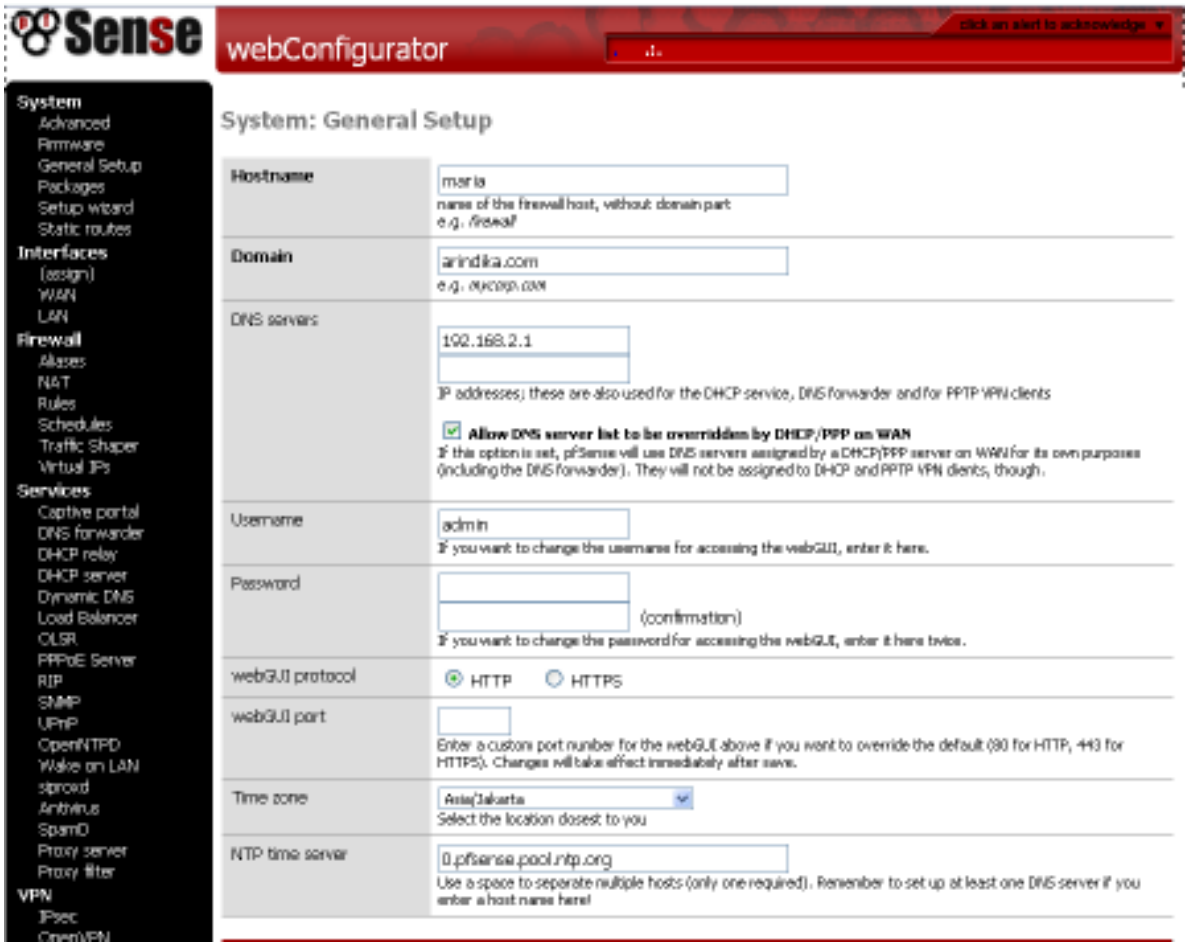
- advance
- firmware
- general setup
- packages
- setup wizard
- static routes

Advanced



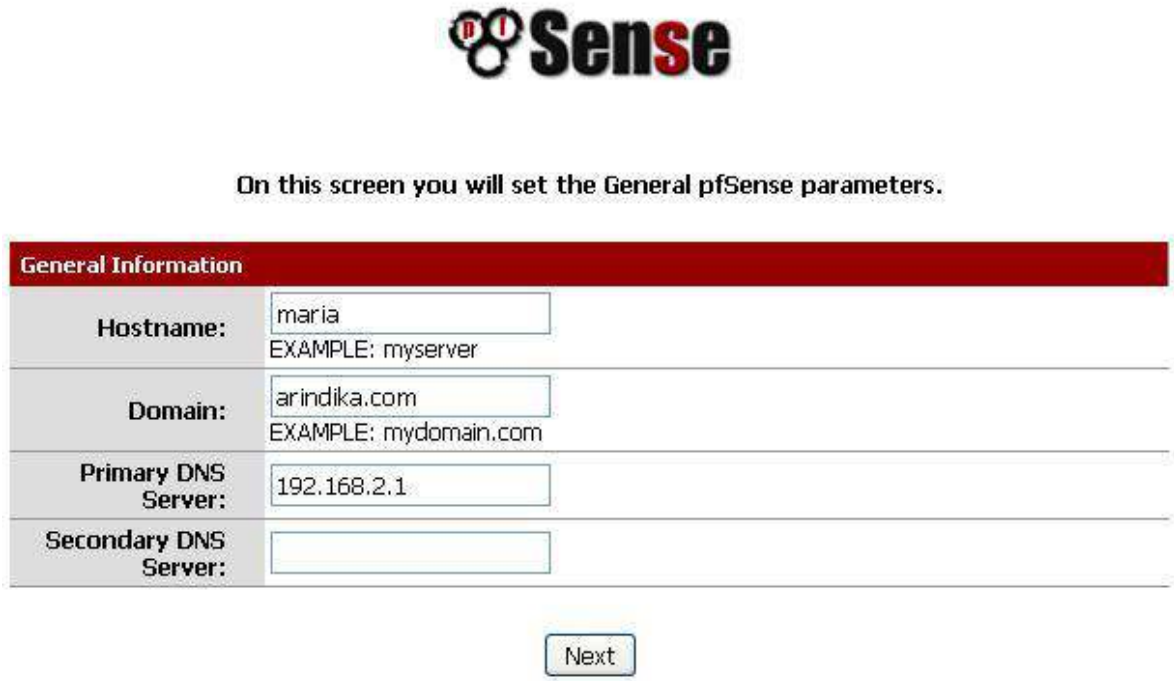
Firmware

General setup



Packages

Setup wizard



Static routes

Interfaces :

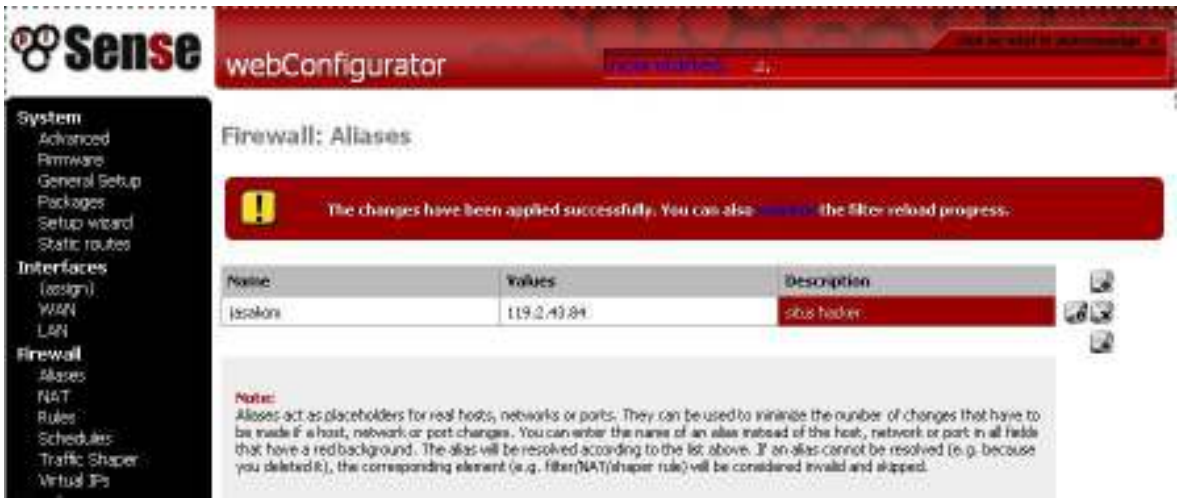
- WAN(interface WAN telah dibahas sebelumnya)
- LAN

LAN

Firewall :

- Aliases
- NAT
- Rules
- Schedules
- Traffic shaper
- Virtual IPs

Aliases

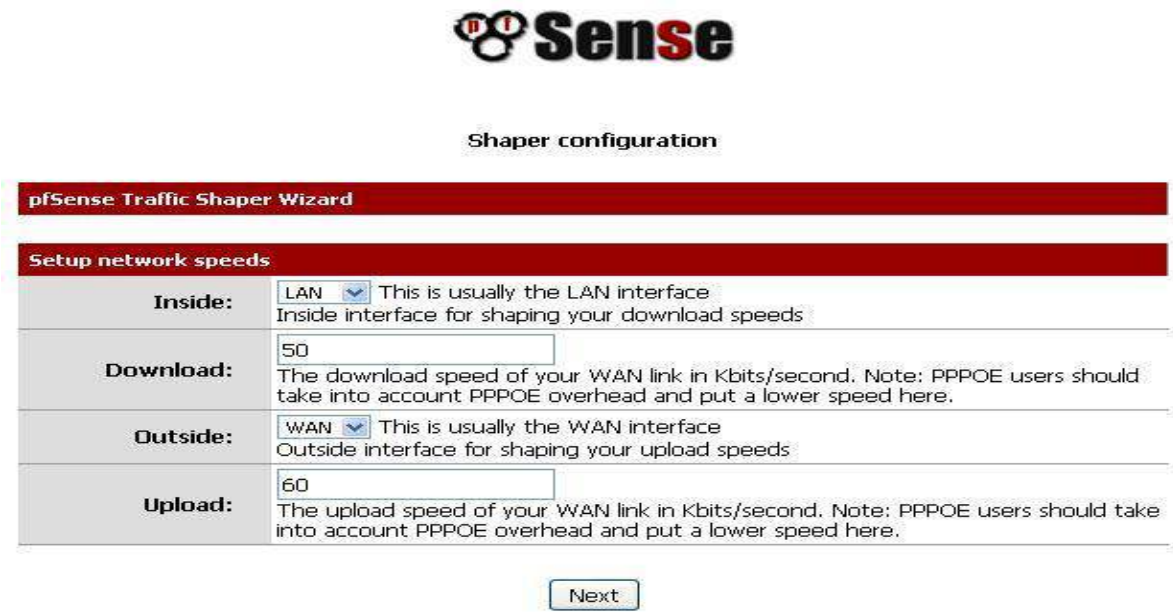


NAT

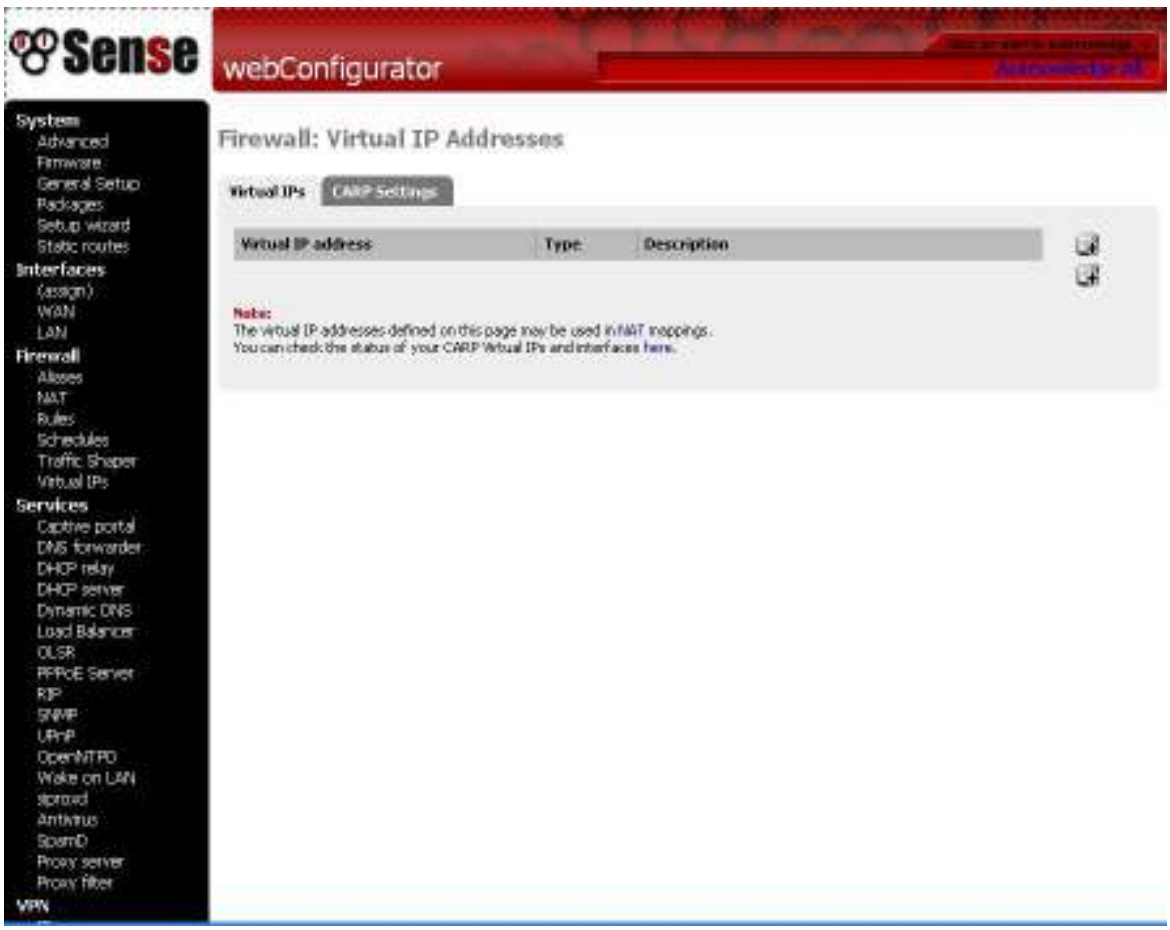
Rules

Schedules

Traffic shaper



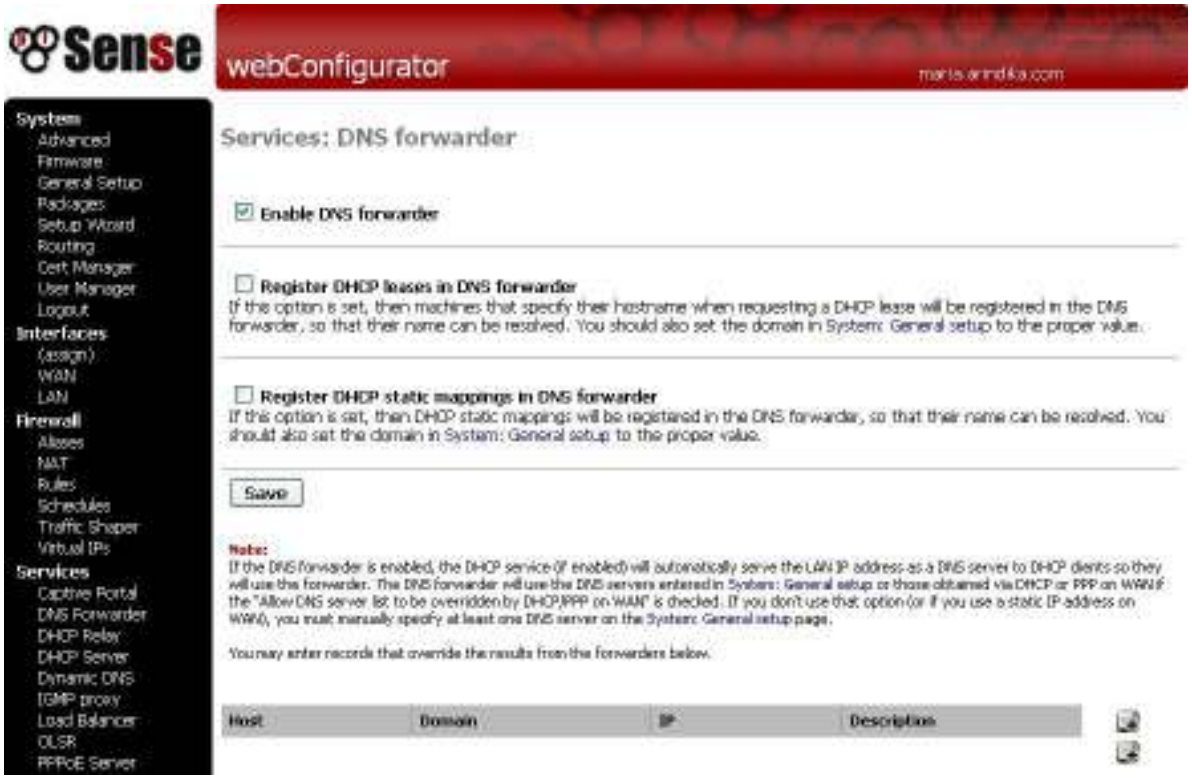
Virtual IPs



Services :

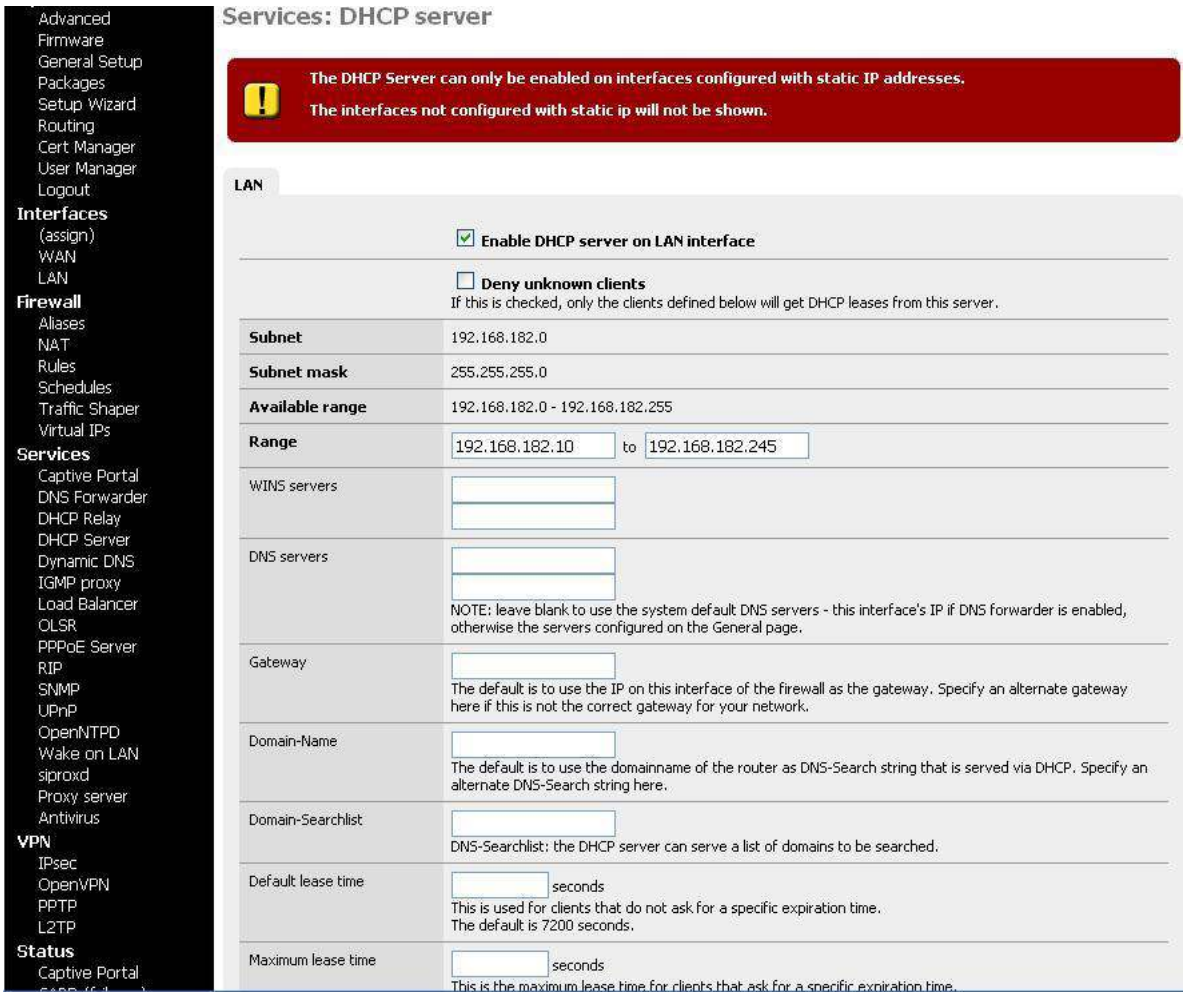
- Captive portal(sudah dibahas)
- DNS forwarder
- DHCP relay
- DHCP server
- Dynamic DNS
- Load balancer
- OLSR
- PPPoE server
- RIP
- SNMP
- UPnP
- OpenNTPD
- Wake on LAN
- Siproxd
- Antivirus
- spamD
- Proxy server
- Proxy filter

DNS forwarder



DHCP relay

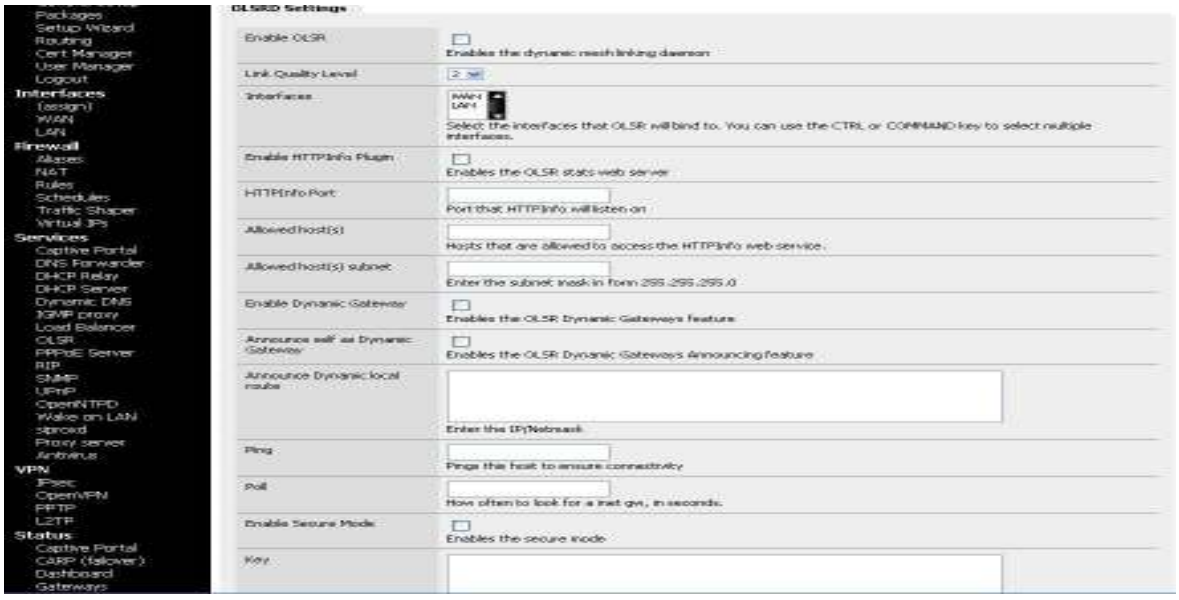
DHCP Server



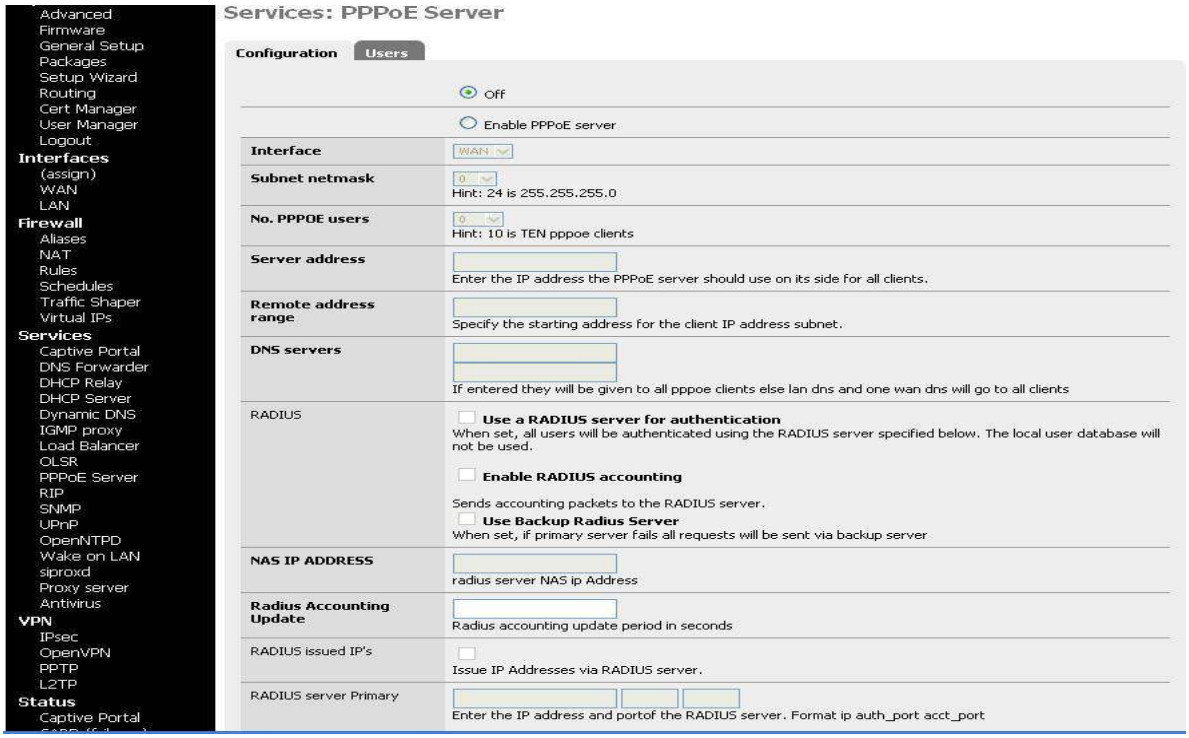
Dynamic DNS

Load balancer

OLSR

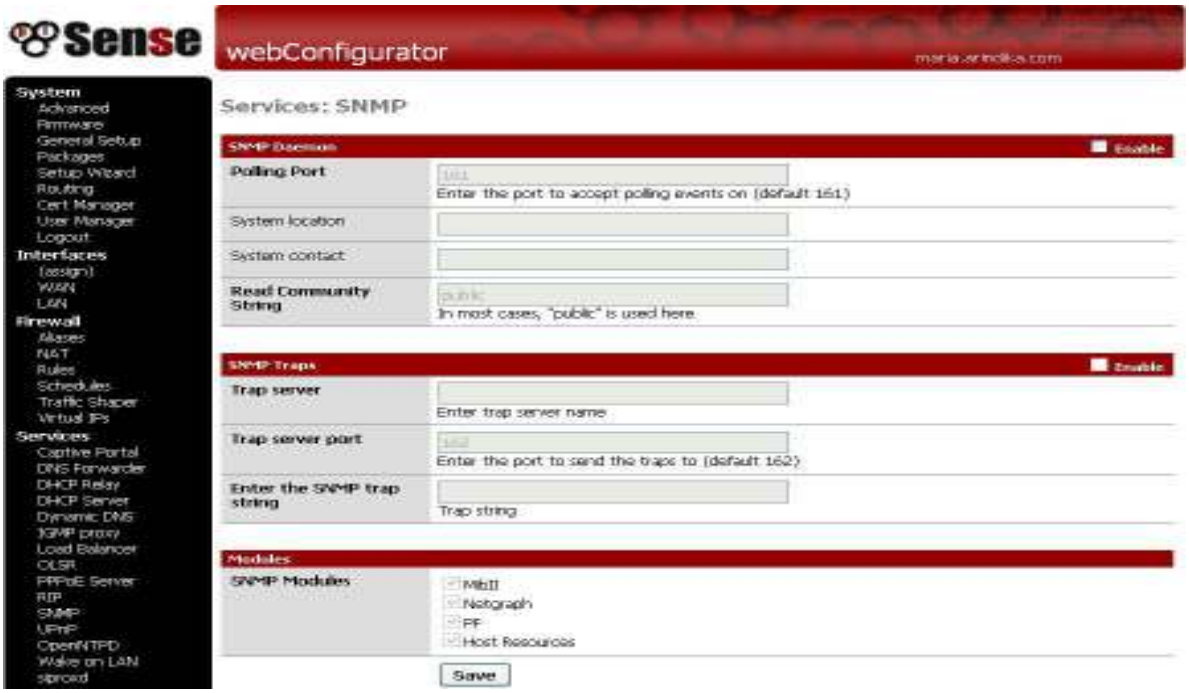


PPPoE server

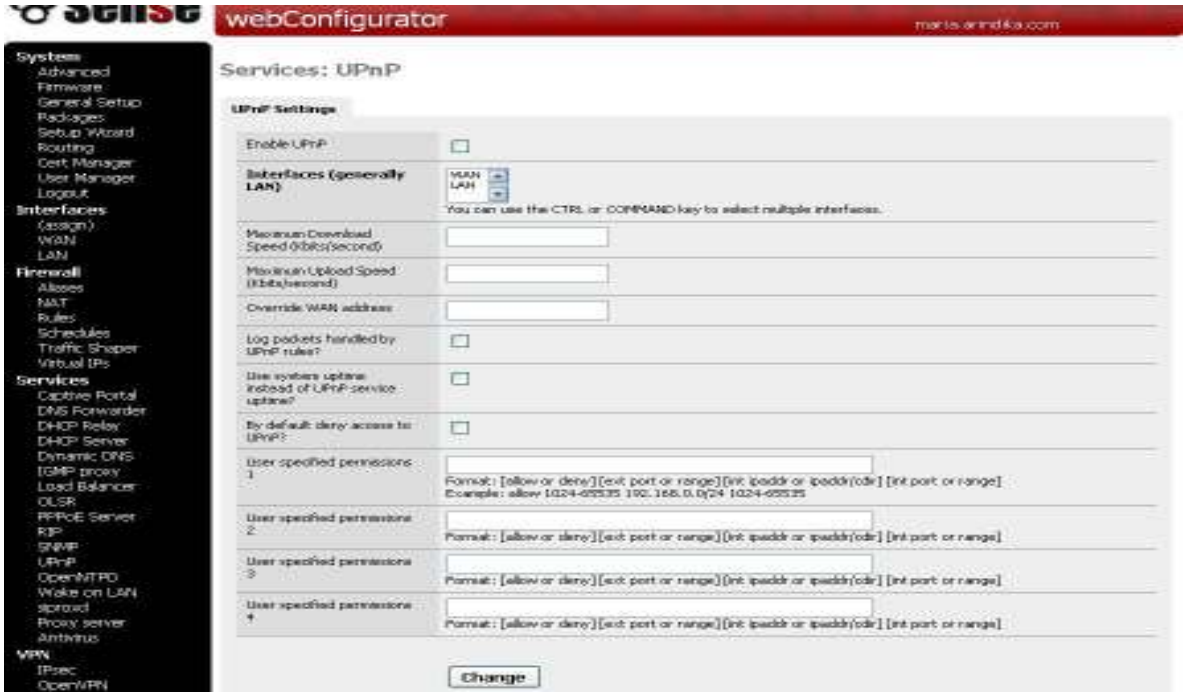


RIP

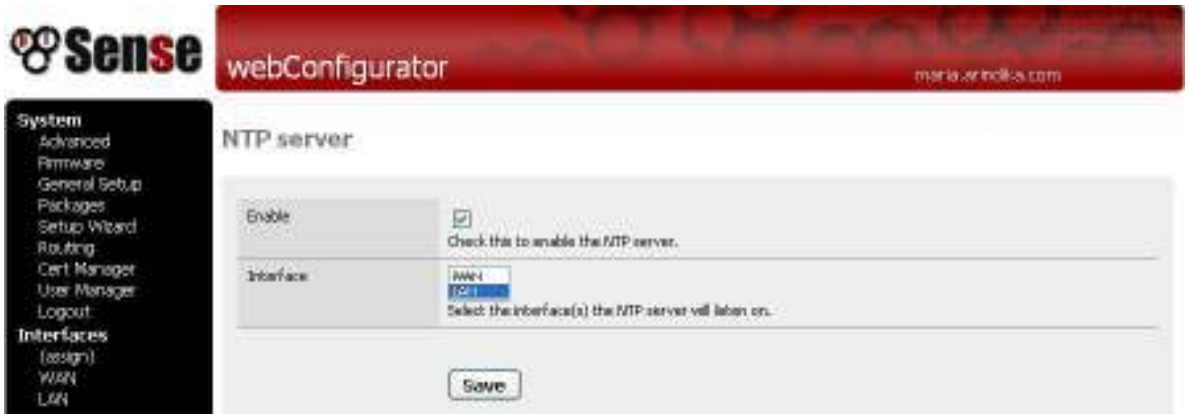
SNMP


Sense
webConfigurator
maria.arindika.com
System
Advanced
Firmware
General Setup
Packages
Setup Wizard
Routing
Cert Manager
User Manager
Logout
Interfaces
(assign)
WAN
LAN
Firewall
Aliases
NAT
Rules
Schedules
Traffic Shaper
Virtual IPs
Services
Captive Portal
DNS Forwarder
DHCP Relay
DHCP Server
Dynamic DNS
IGMP proxy
Load Balancer
OLSR
PPPoE Server
RIP
SNMP
UPnP
OpenNTPD
Wake on LAN
sproxd
Services: SNMP
SNMP Daemon
Enable
Polling Port
161
Enter the port to accept polling events on (default 161)
System location
System contact
Read Community String
public
In most cases, "public" is used here
SNMP Traps
Enable
Trap server
Enter trap server name
Trap server port
162
Enter the port to send the traps to (default 162)
Enter the SNMP trap string
Trap string
Modules
SNMP Modules
MibII
Netgraph
PF
Host Resources
Save

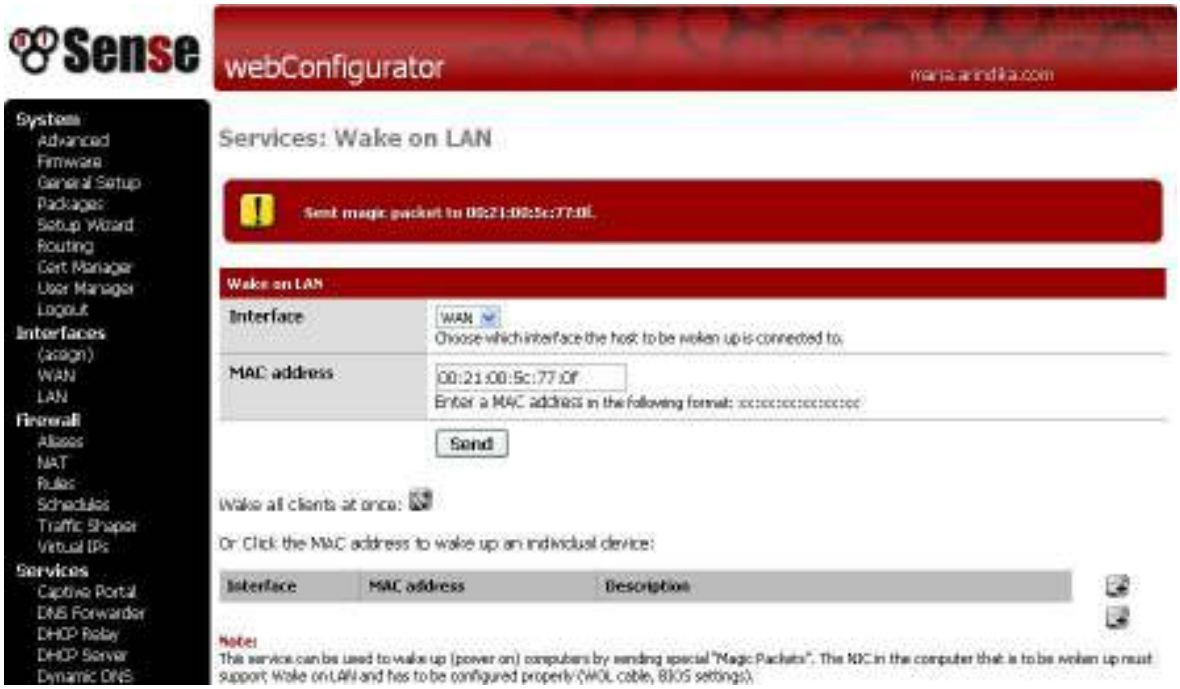
UPnP


webConfigurator
maria.arindika.com
System
Advanced
Firmware
General Setup
Packages
Setup Wizard
Routing
Cert Manager
User Manager
Logout
Interfaces
(assign)
WAN
LAN
Firewall
Aliases
NAT
Rules
Schedules
Traffic Shaper
Virtual IPs
Services
Captive Portal
DNS Forwarder
DHCP Relay
DHCP Server
Dynamic DNS
IGMP proxy
Load Balancer
OLSR
PPPoE Server
RIP
SNMP
UPnP
OpenNTPD
Wake on LAN
sproxd
Proxy server
Antivirus
VPN
IPsec
OpenVPN
Services: UPnP
UPnP Settings
Enable UPnP
Interfaces (generally LAN)
WAN
LAN
You can use the CTRL or COMMAND key to select multiple interfaces.
Maximum Download Speed (Kbits/second)
Maximum Upload Speed (Kbits/second)
Override WAN address
Log packets handled by UPnP rules?
Use system uptime instead of UPnP service uptime?
By default deny access to UPnP?
User specified permissions 1
Format: [allow or deny] [ext port or range] [int ipaddr or ipaddr/cdr] [int port or range]
Example: allow 1024-65535 192.168.0.0/24 1024-65535
User specified permissions 2
User specified permissions 3
User specified permissions 4
Change

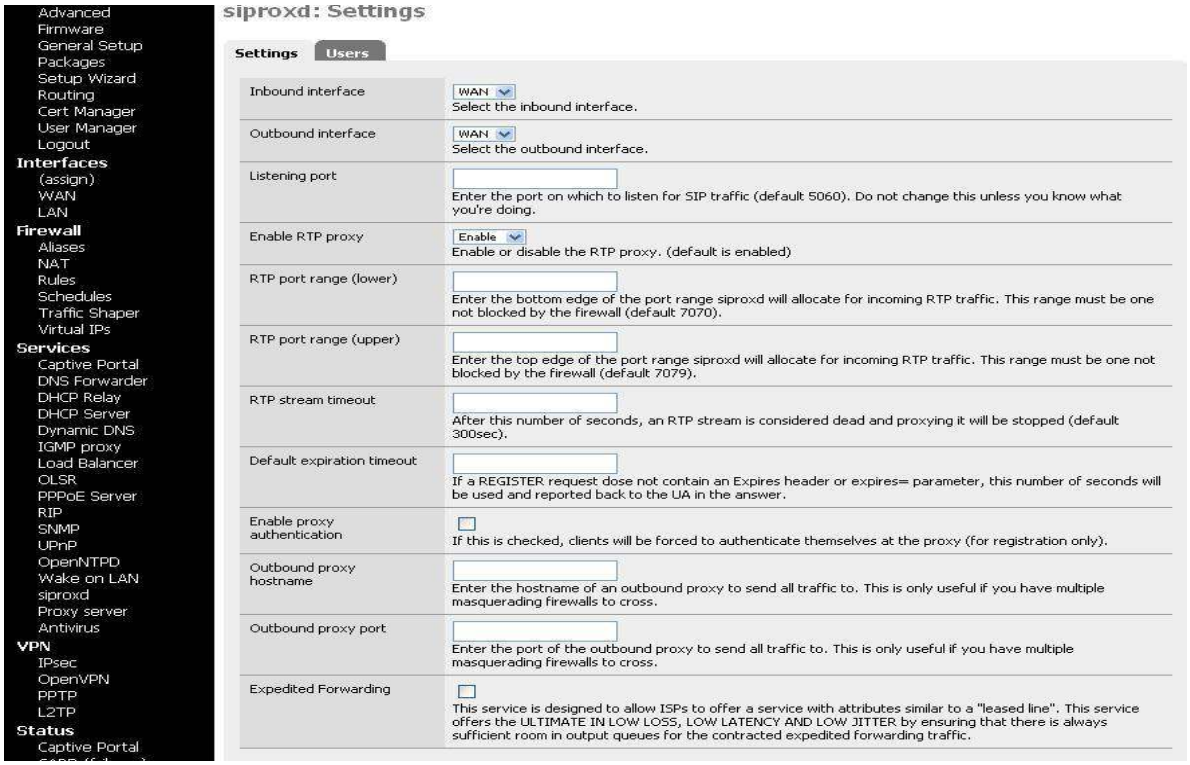
OpenNTPD



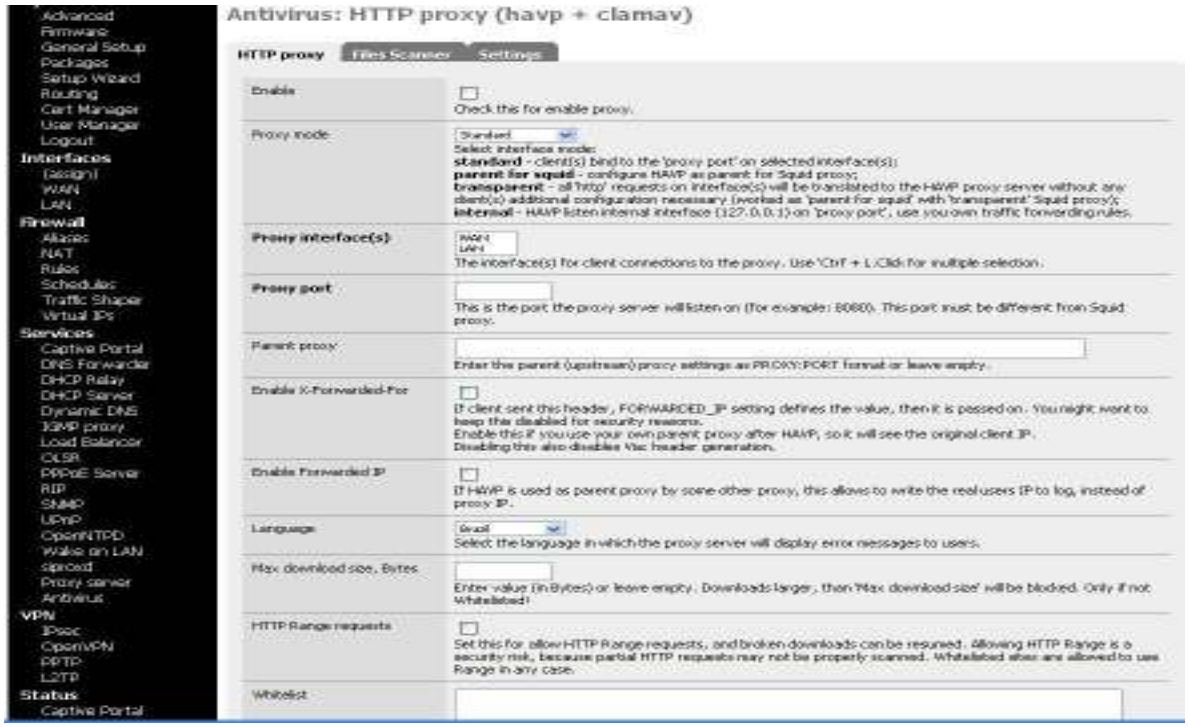
Wake on LAN



Siproxd

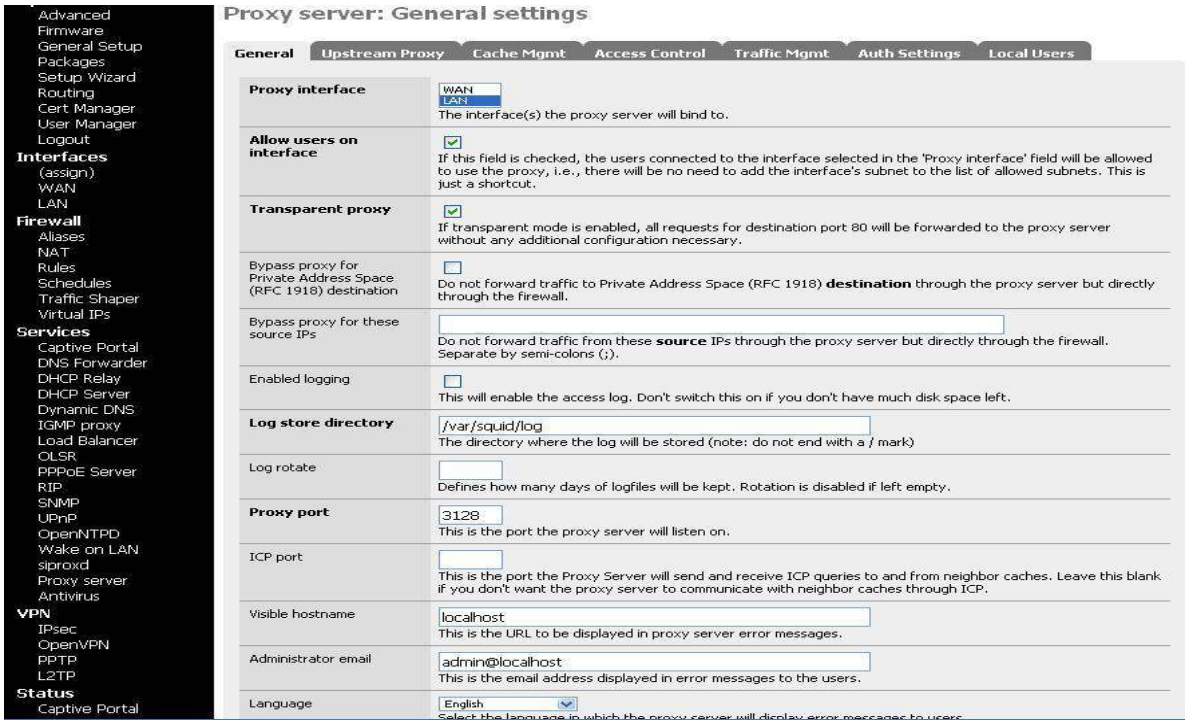


Antivirus



spamD

Proxy server



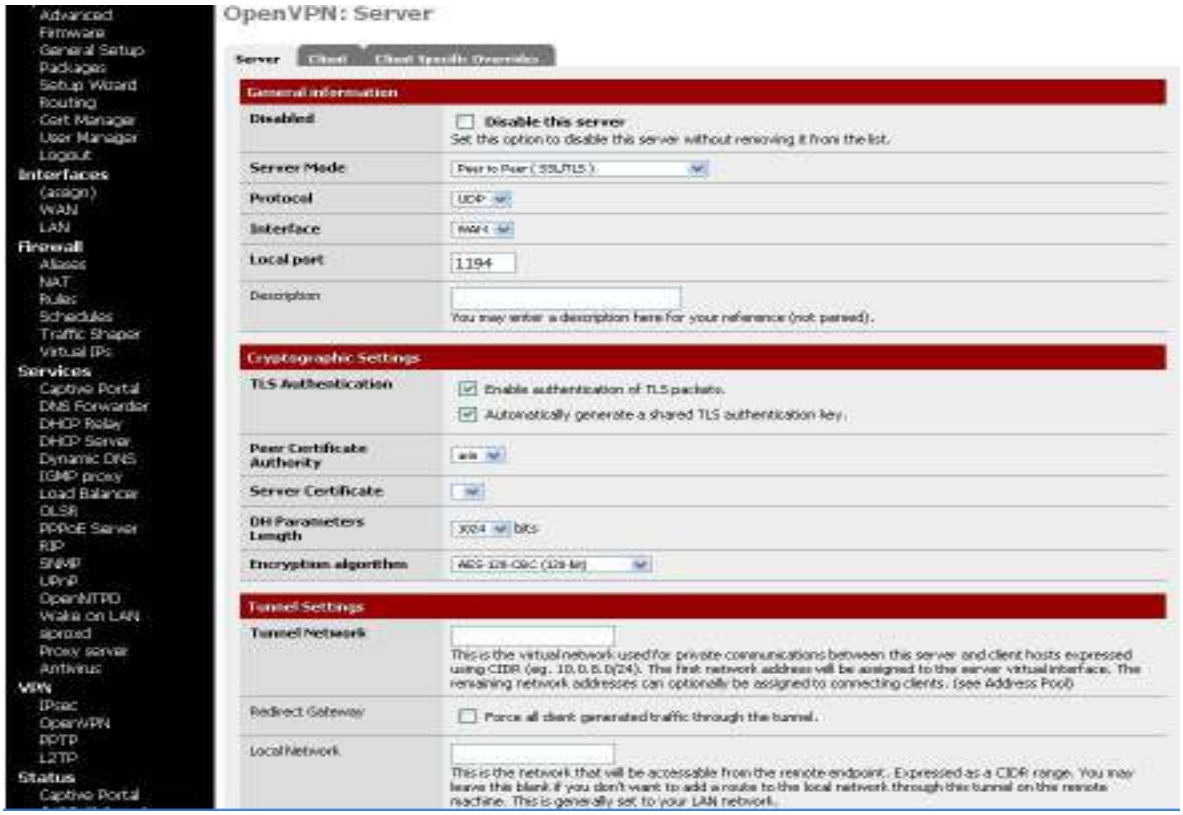
Proxy filter

VPN :

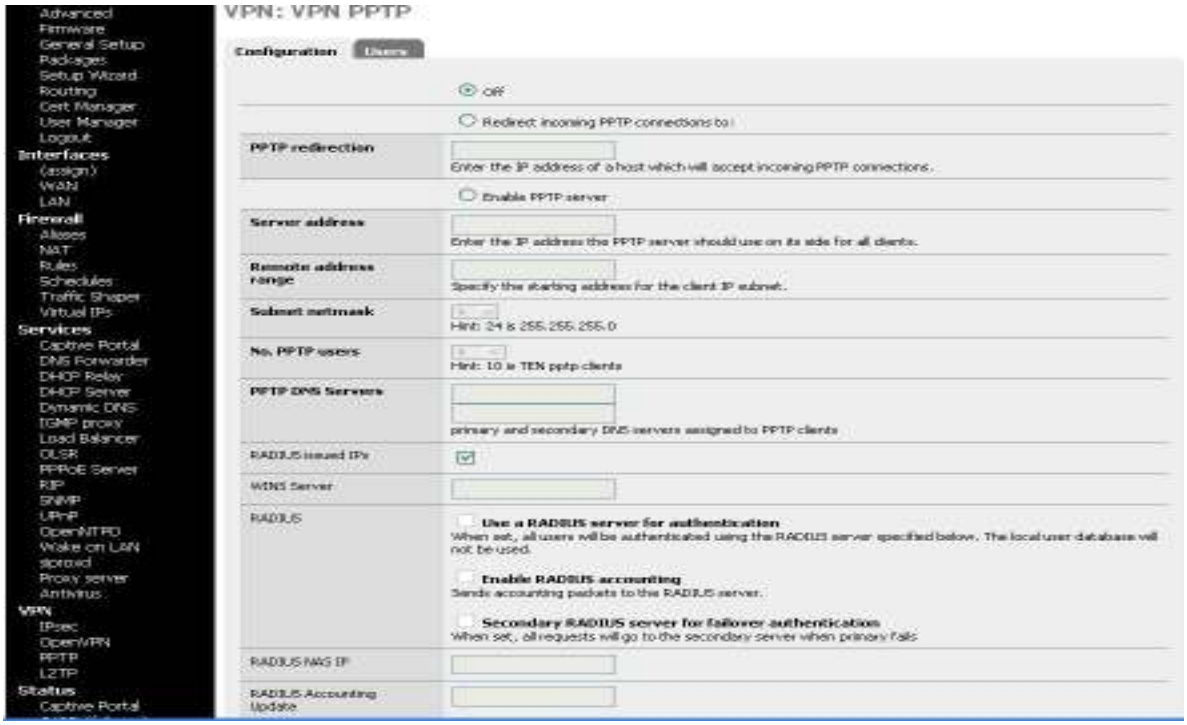
- IPsec
- Open VPN
- PPTP
- L2TP

IPsec

Open VPN



PPTP



Status :

- Captive portal
- CARP (failover)
- DHCP leases
- Filter reload status
- Interfaces
- IPsec
- Load balancer
- Package logs
- Queues
- RRD Graphs
- Services
- System
- System logs
- Traffic graph
- UPnP

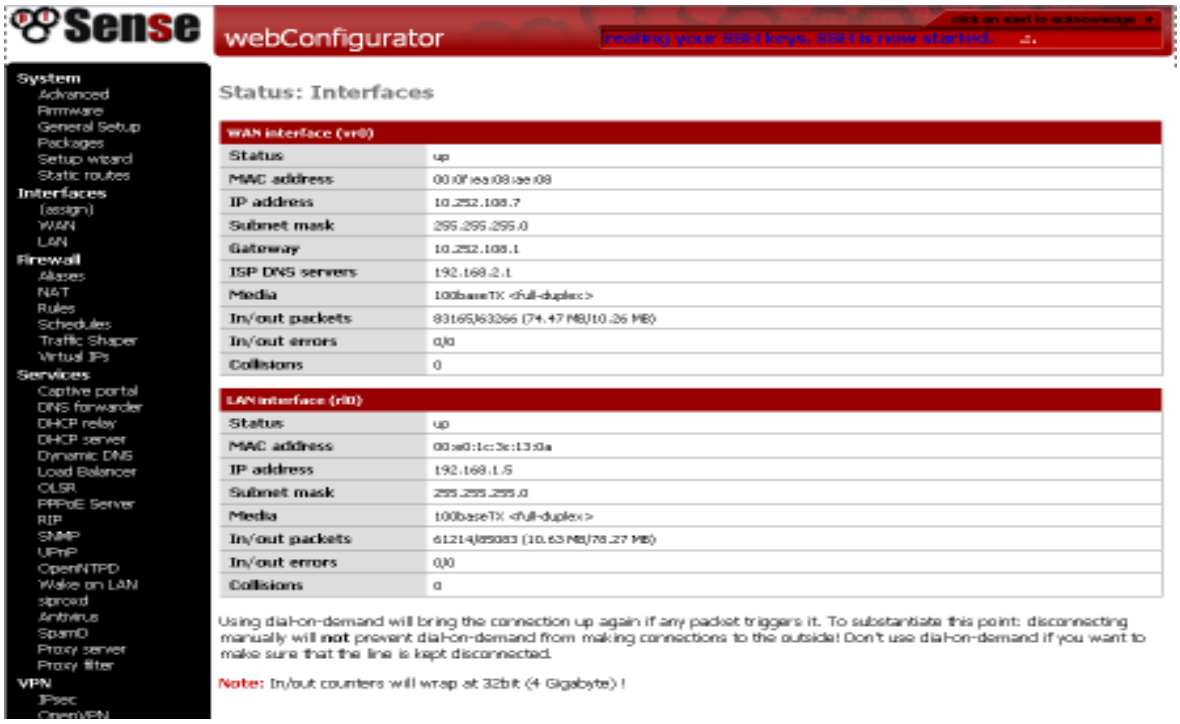
Captive portal

CARP(failover)

DHCP leases

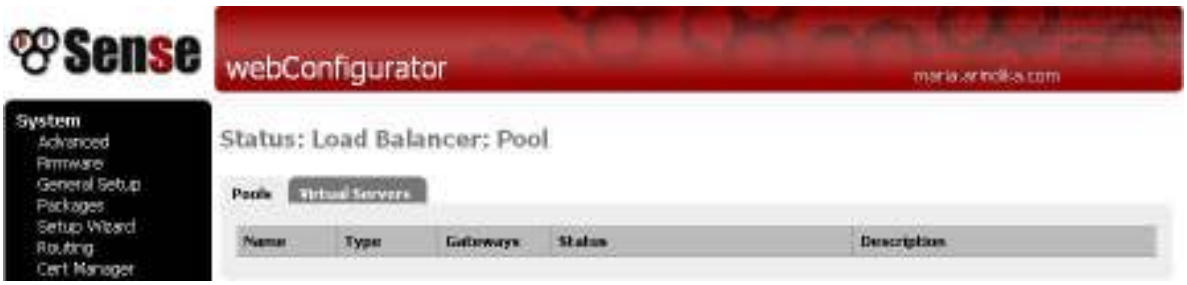
Filter reload

Interfaces

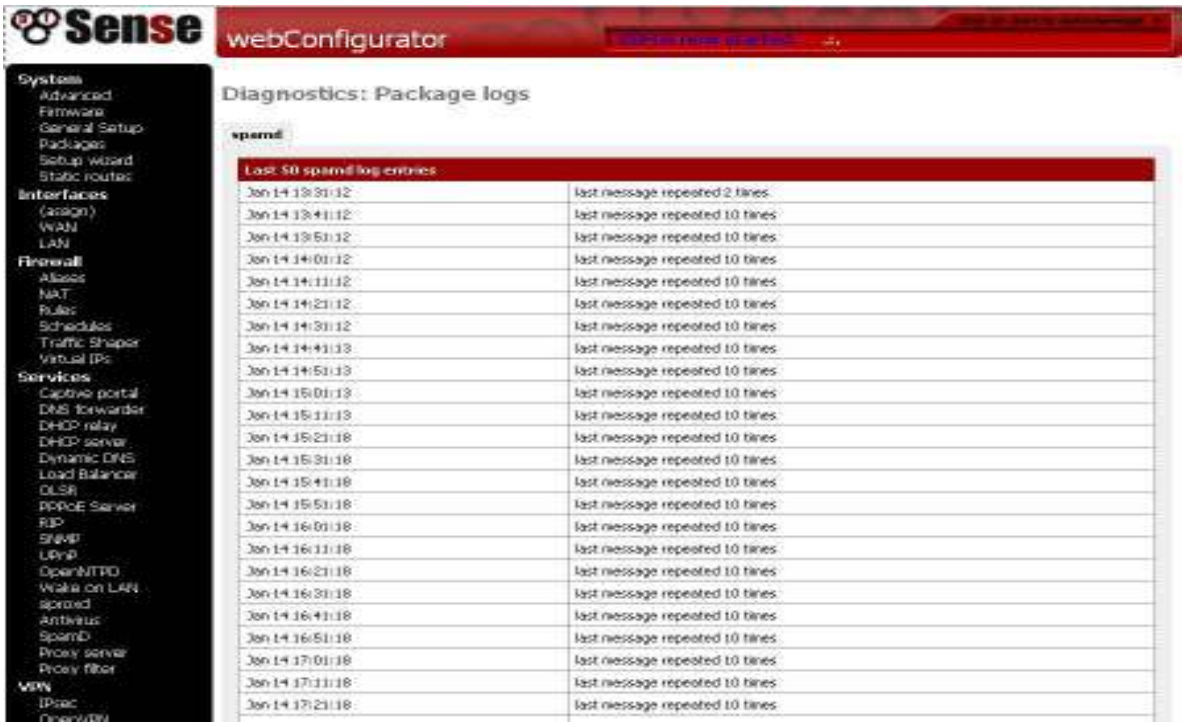


IPsec

Load balancer

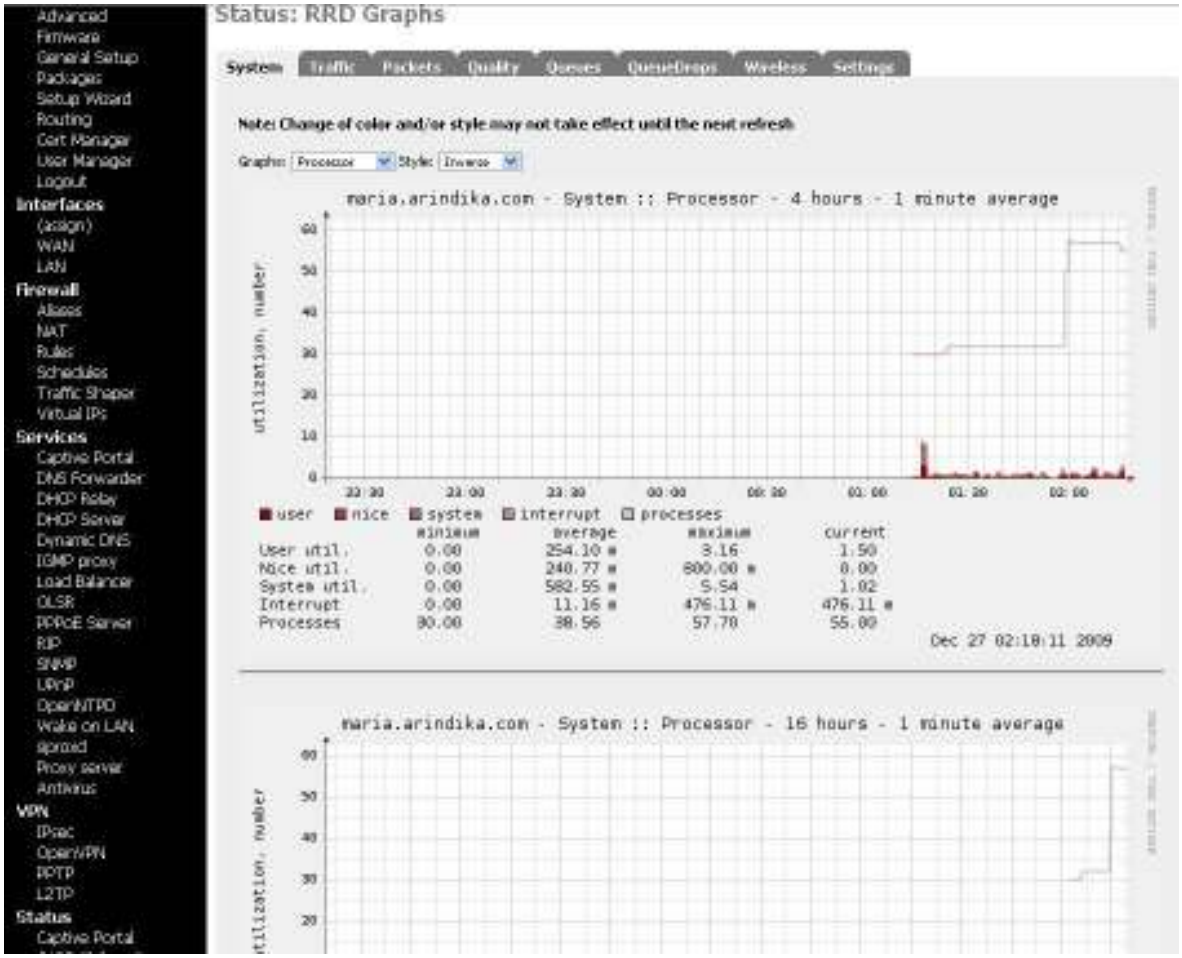


Packages logs

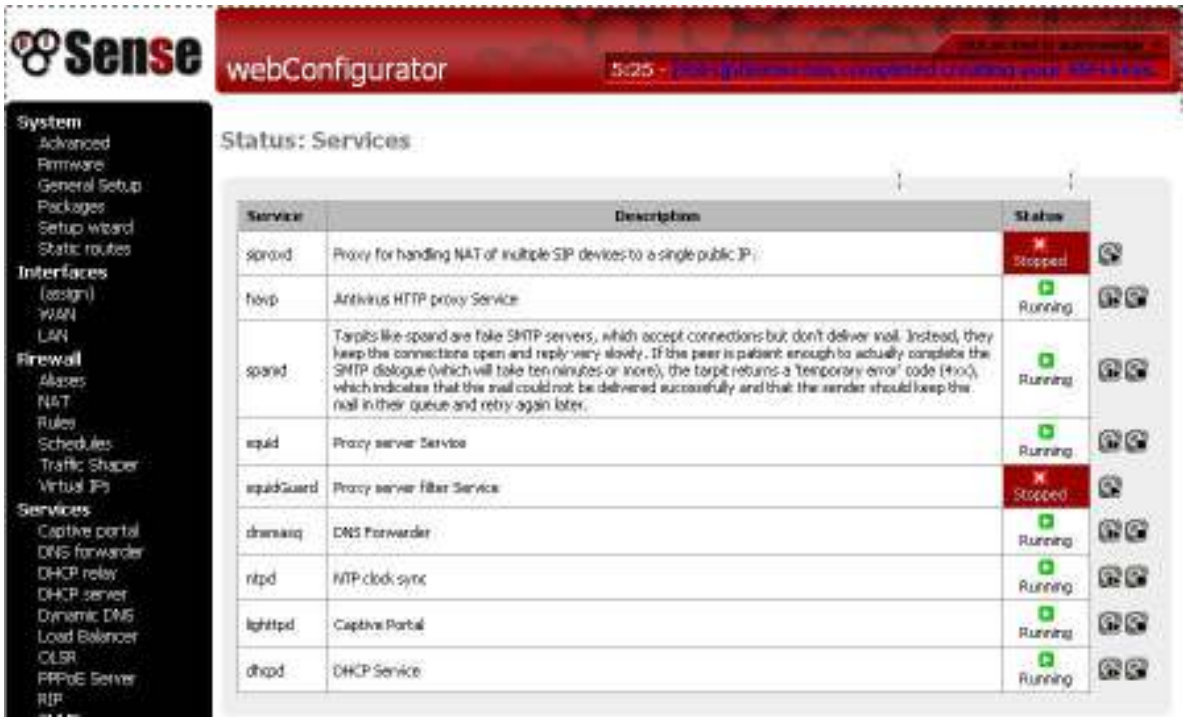


Queues

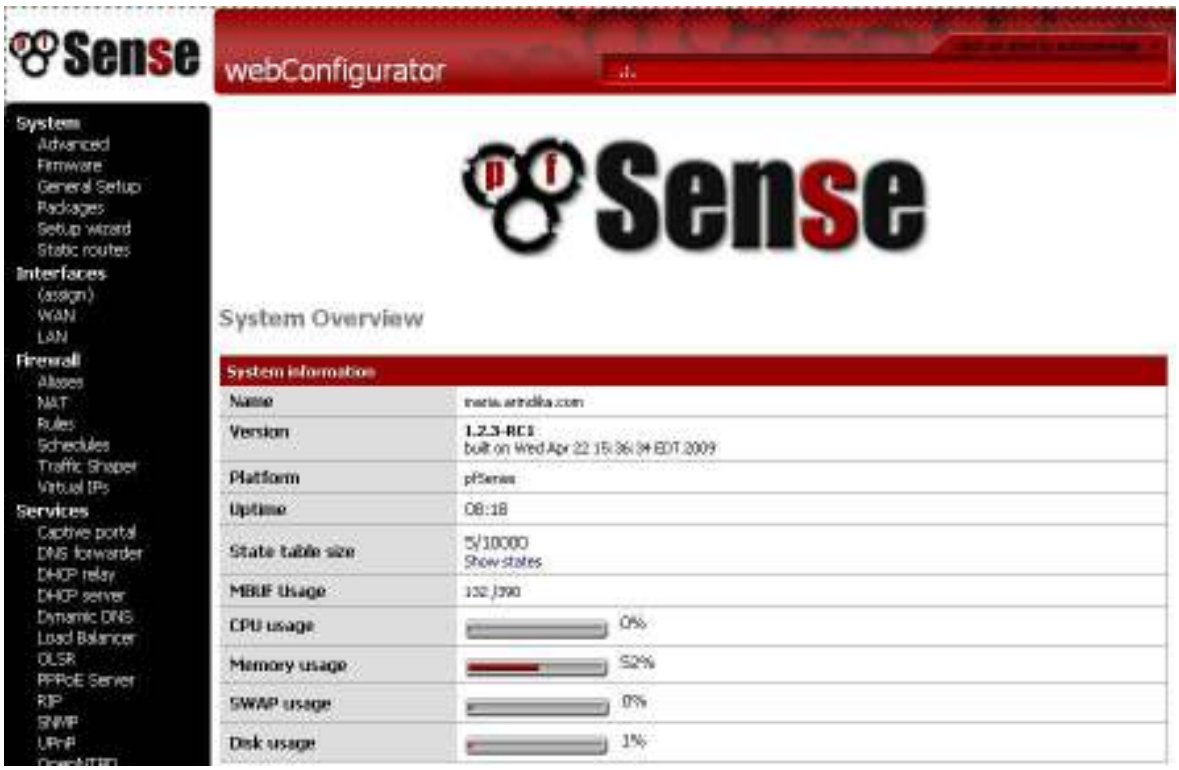
RRD Graphs



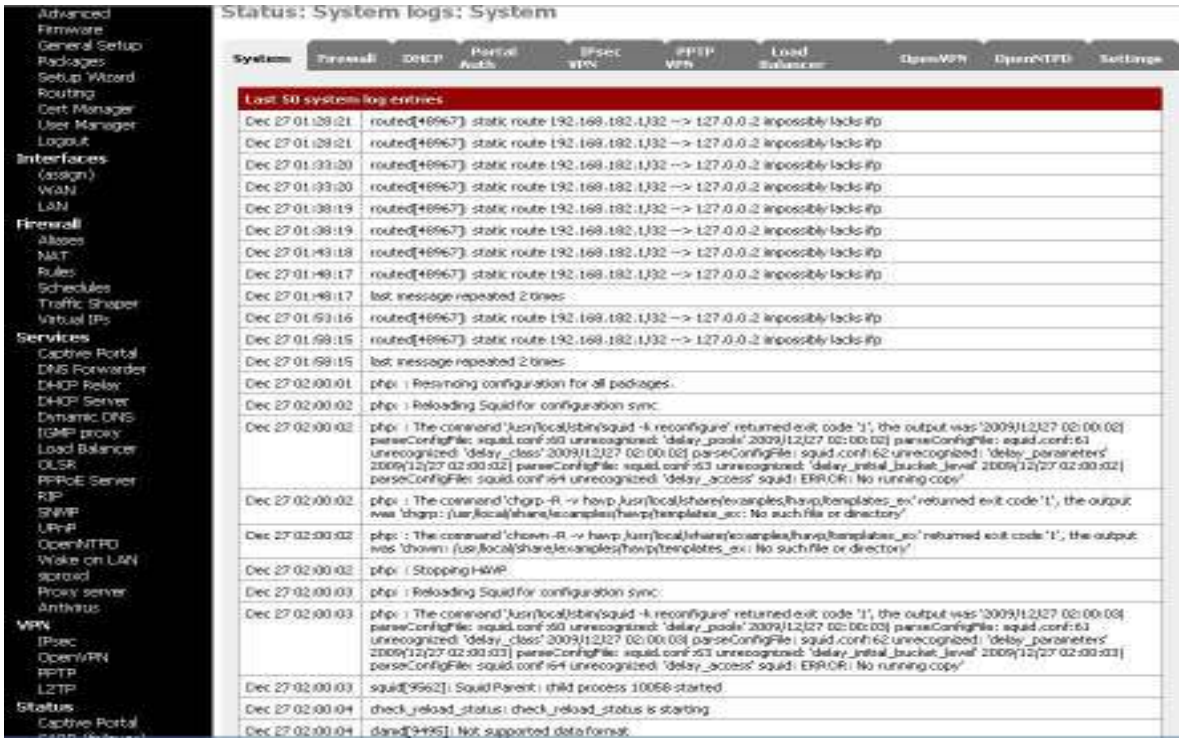
Services



System



System logs



Traffic graph

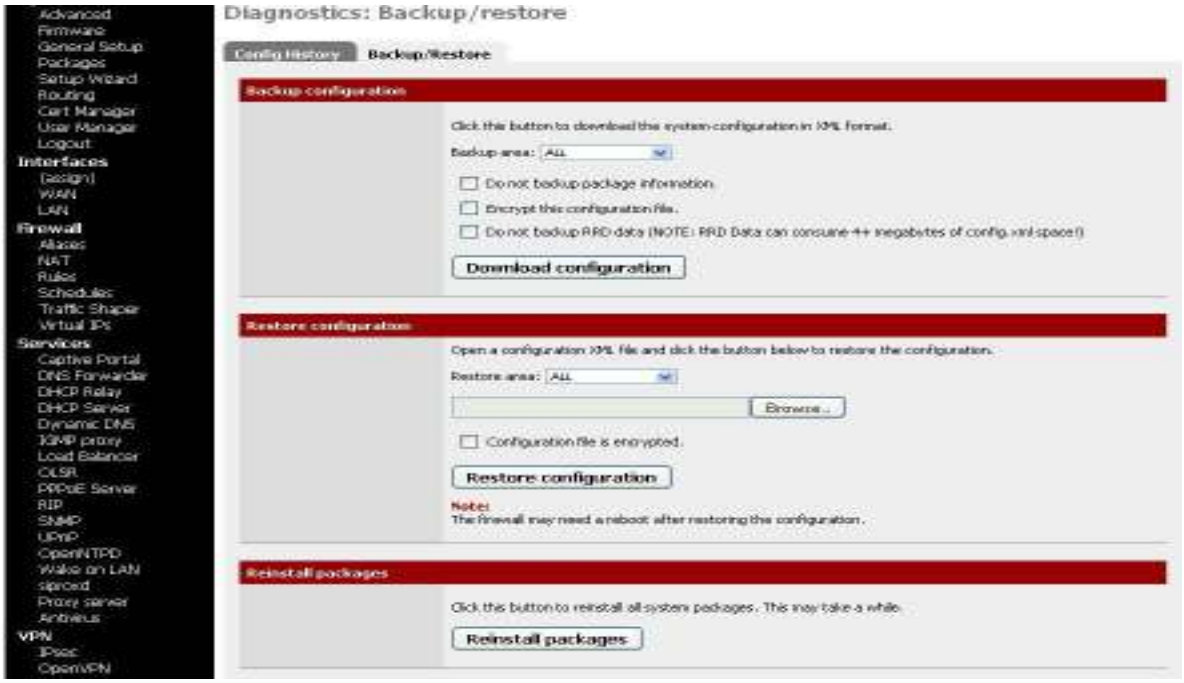
UPnP

Diagnostics :

- ARP tables
- Backup/restore
- Command prompt
- Edit file
- Factory defaults
- Halt system
- Ping
- Reboot system
- Routes
- States
- Traceroute
- Packet capture

Arp table

Backup/restore



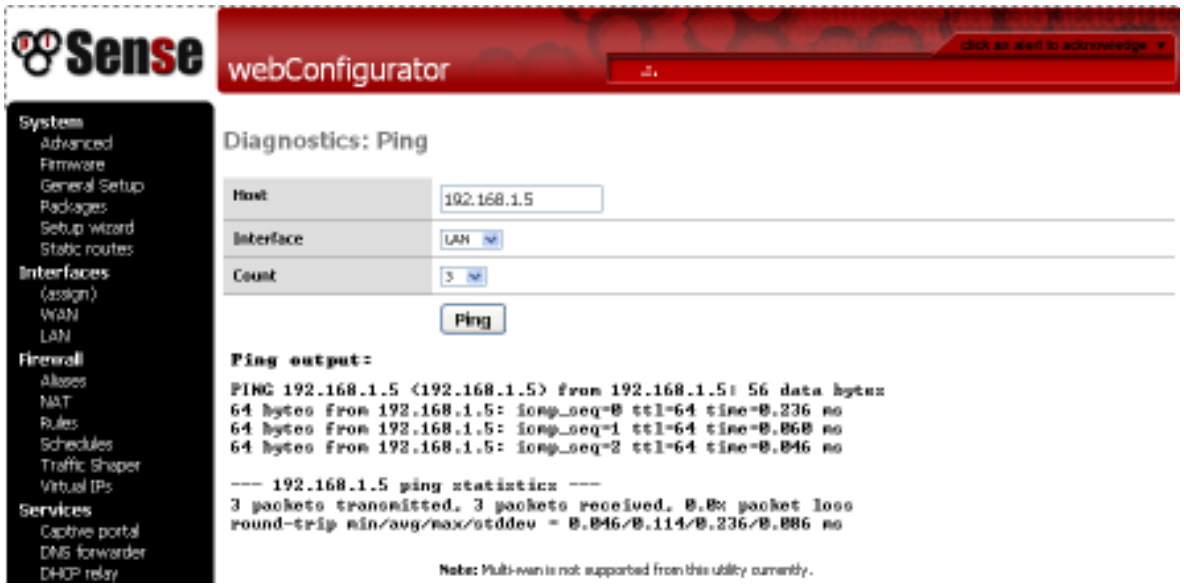
Command prompt

Edit file

Factory defaults

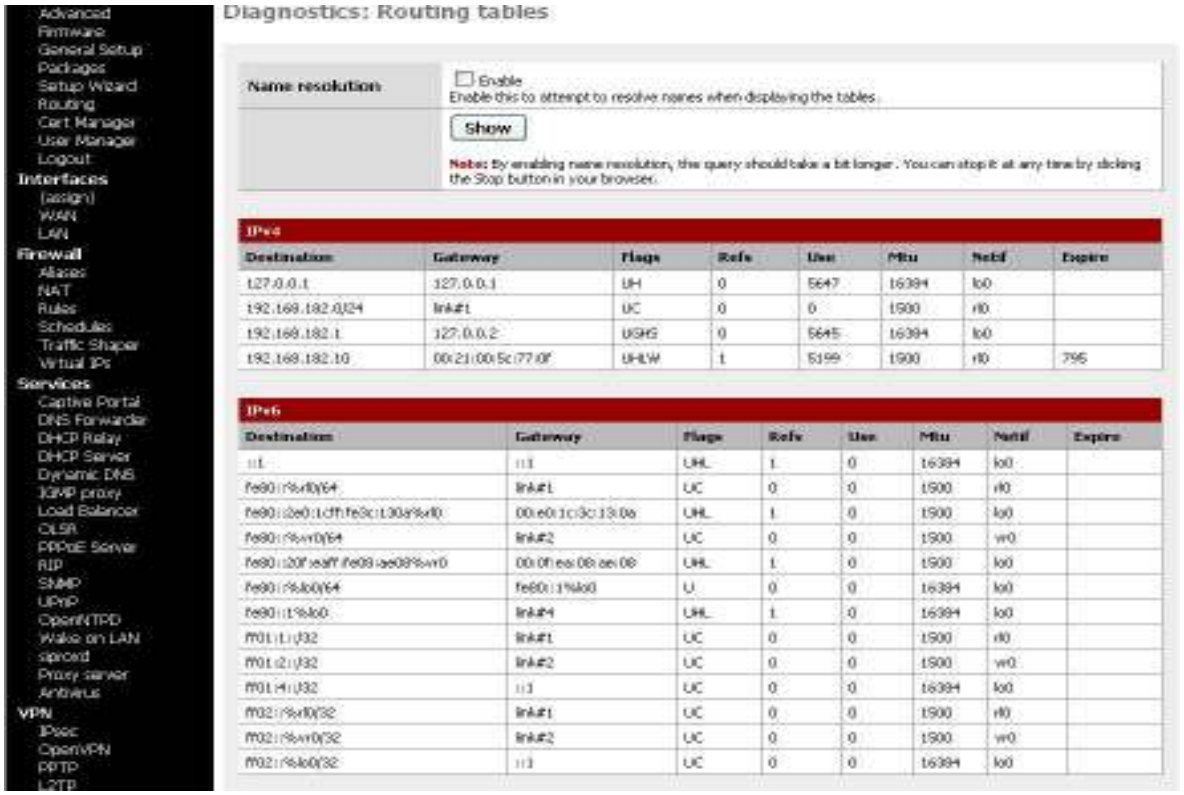
Halt system

Ping



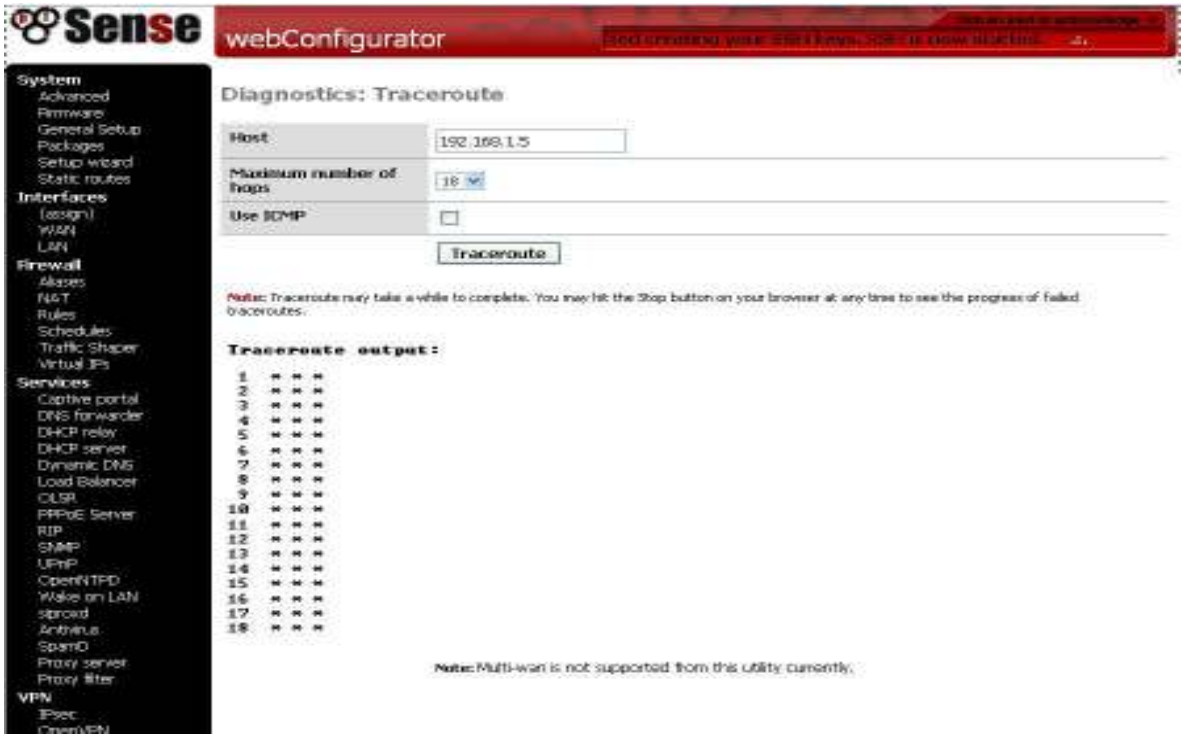
Reboot system

Routes

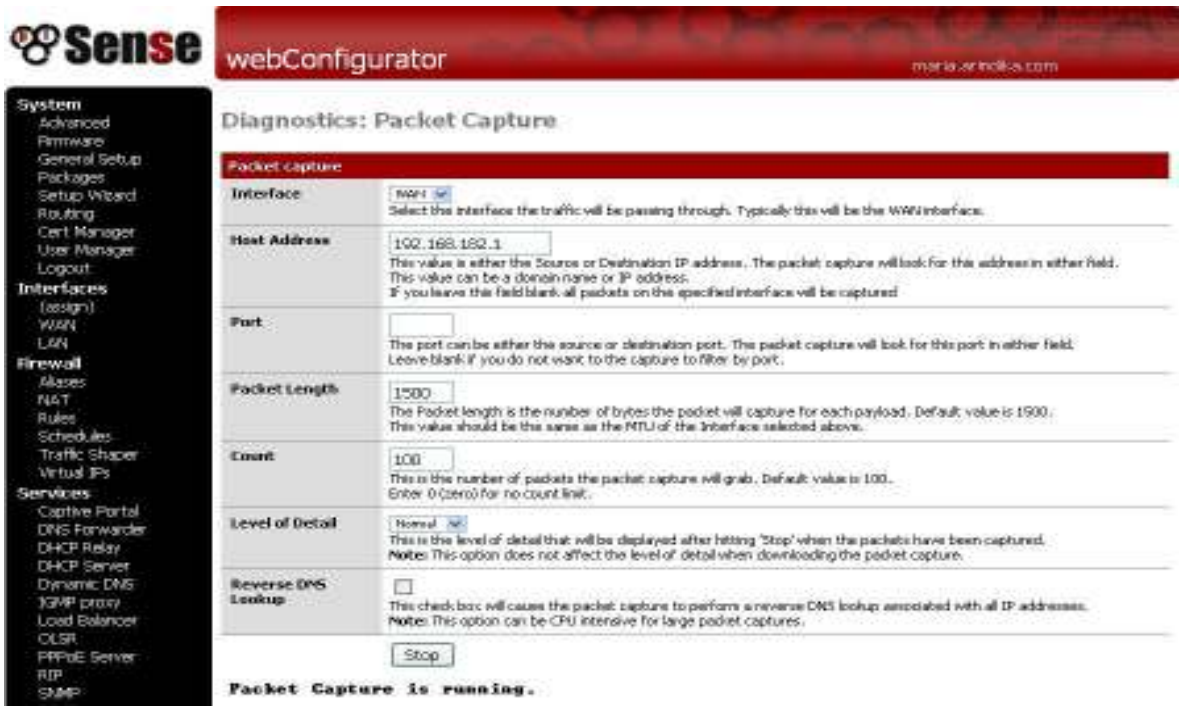


states

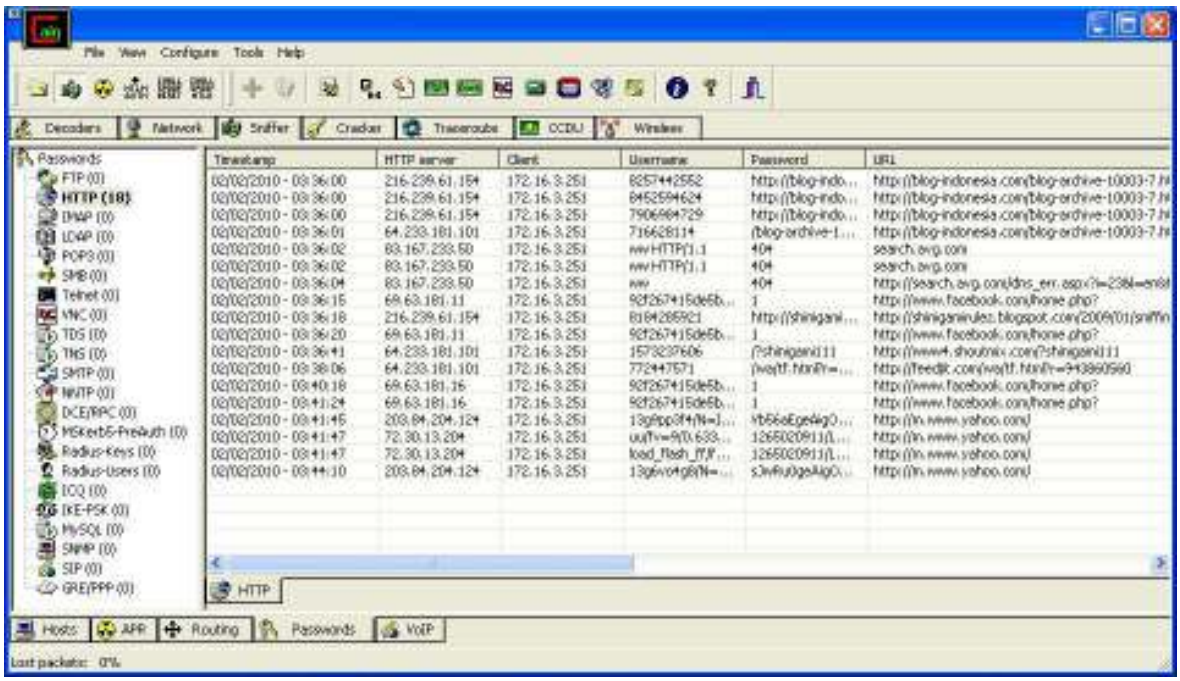
Traceroute



Packet capture



Seperti halnya pengujian menggunakan software cain & able yang dilakukan sebelumnya pada software monowall, proses pengujian aktifitas sniffing pada pfsense berhasil mengetahui situs yang sedang diakses, namun tidak berhasil menampilkan password pengguna

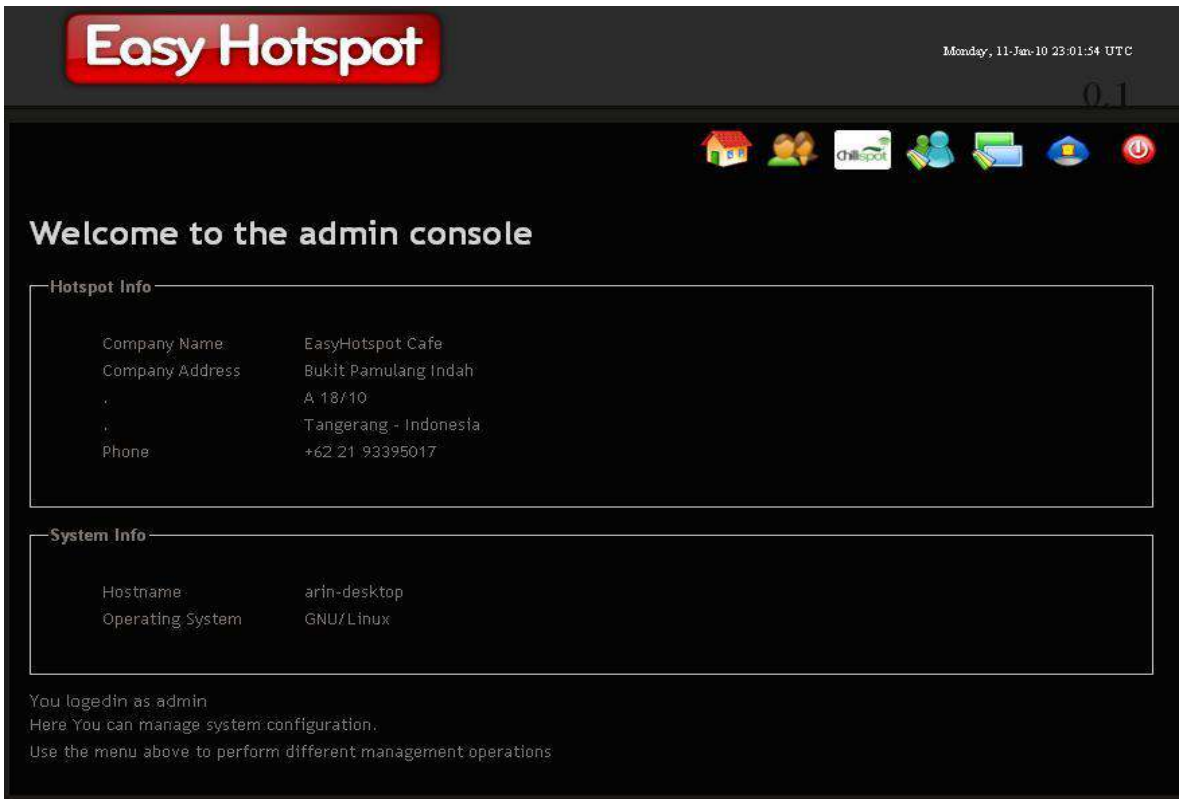


3.1 Easy Hotspot

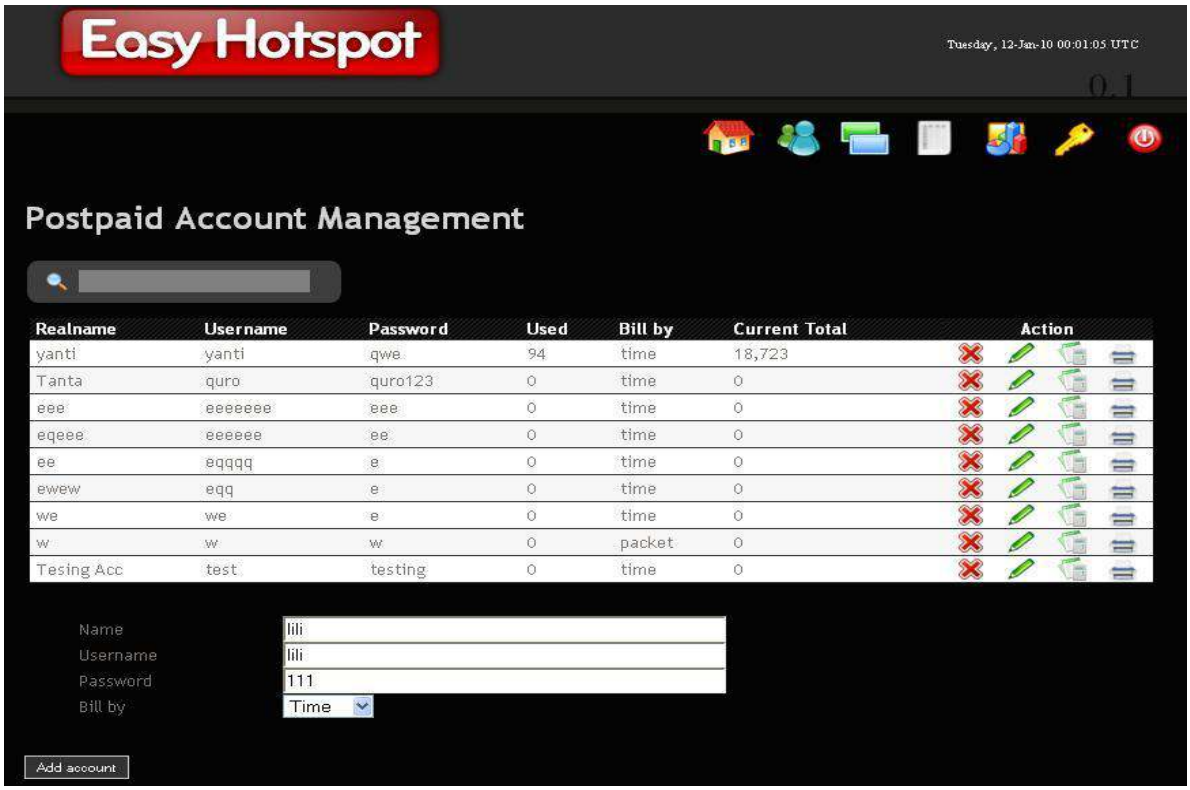
Proses konfigurasi easyhotspot tidak terlalu sulit karena dapat langsung dimanfaatkan untuk manajemen hotspot. Berikut merupakan tampilan login easy hotspot

Login admin

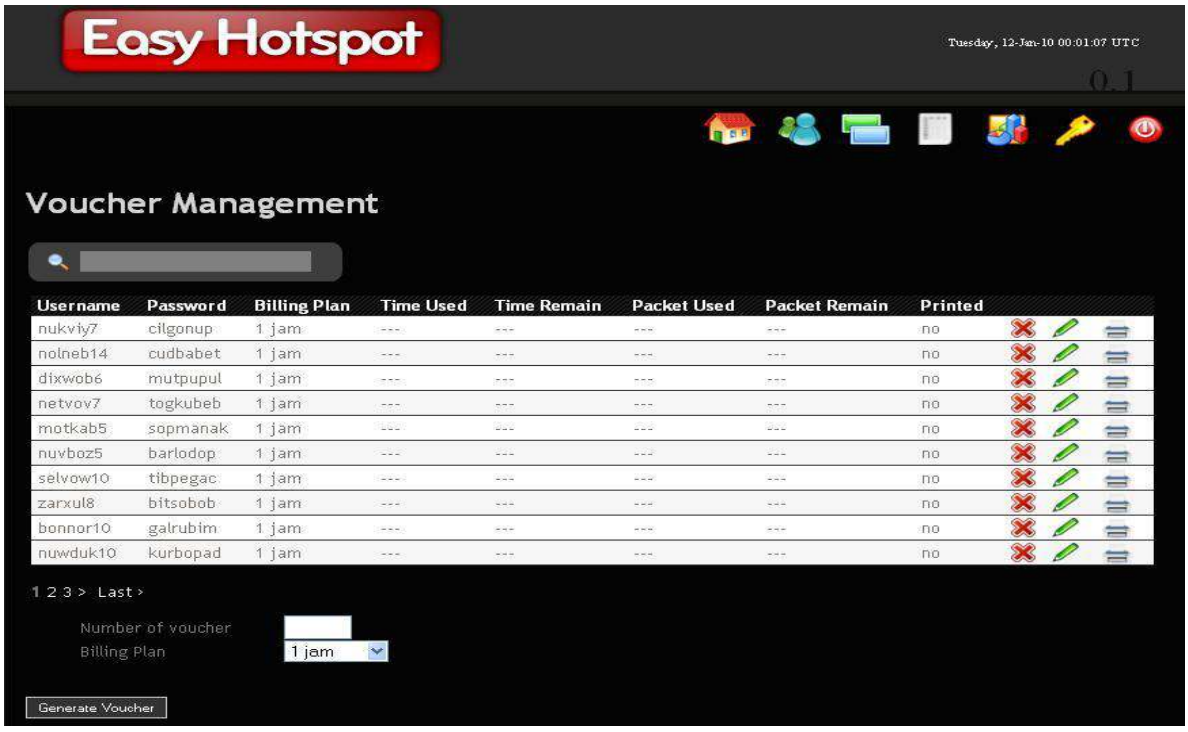
Tampilan Menu admin



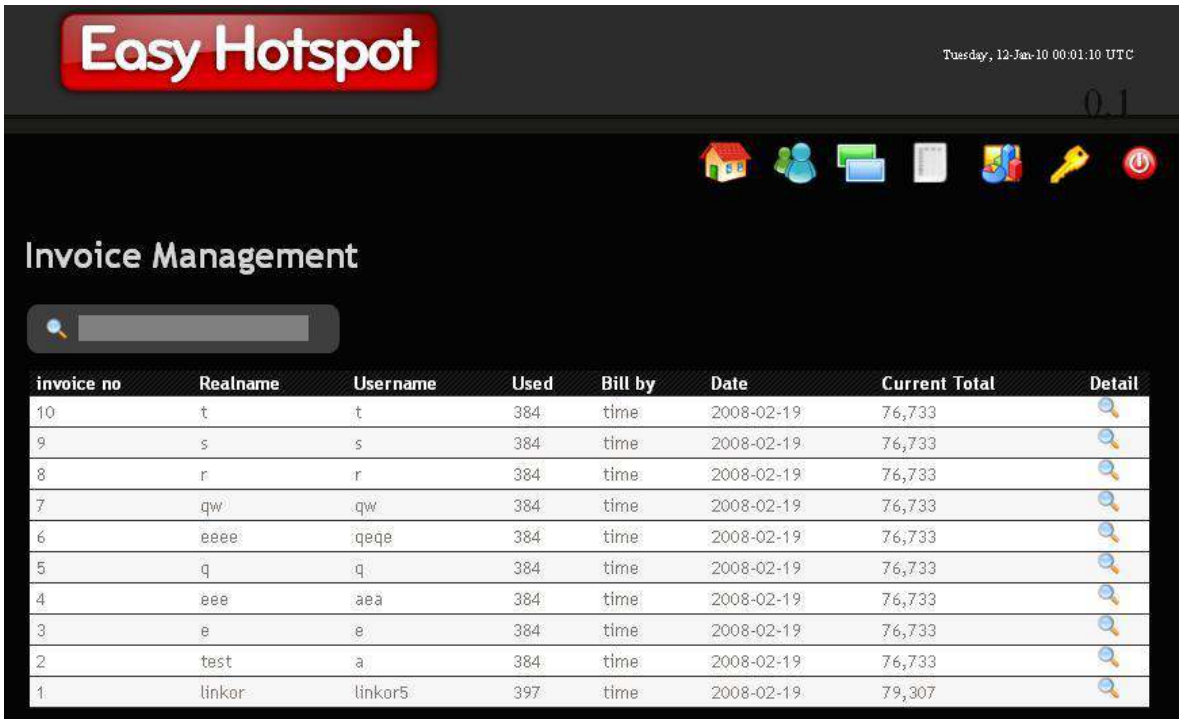
Postapaid account



Voucher account

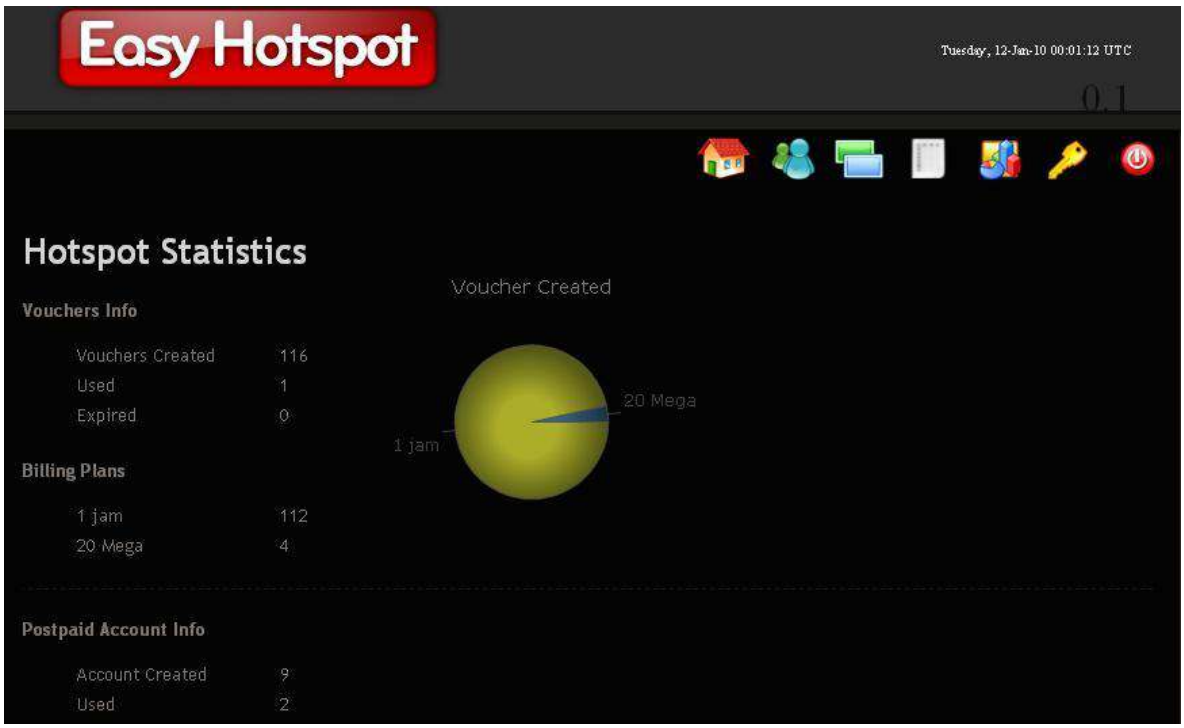


Invoice management

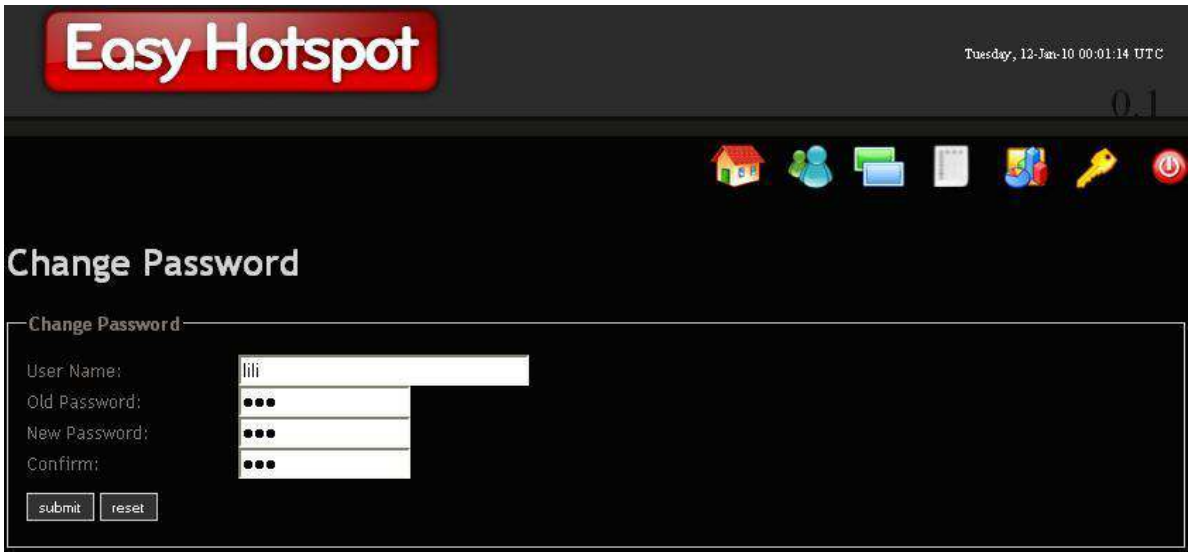


invoice no	Realname	Username	Used	Bill by	Date	Current Total	Detail
10	t	t	384	time	2008-02-19	76,733	
9	s	s	384	time	2008-02-19	76,733	
8	r	r	384	time	2008-02-19	76,733	
7	qw	qw	384	time	2008-02-19	76,733	
6	eeee	qeqe	384	time	2008-02-19	76,733	
5	q	q	384	time	2008-02-19	76,733	
4	eee	aea	384	time	2008-02-19	76,733	
3	e	e	384	time	2008-02-19	76,733	
2	test	a	384	time	2008-02-19	76,733	
1	linkor	linkor5	397	time	2008-02-19	79,307	

Hotspot satistic



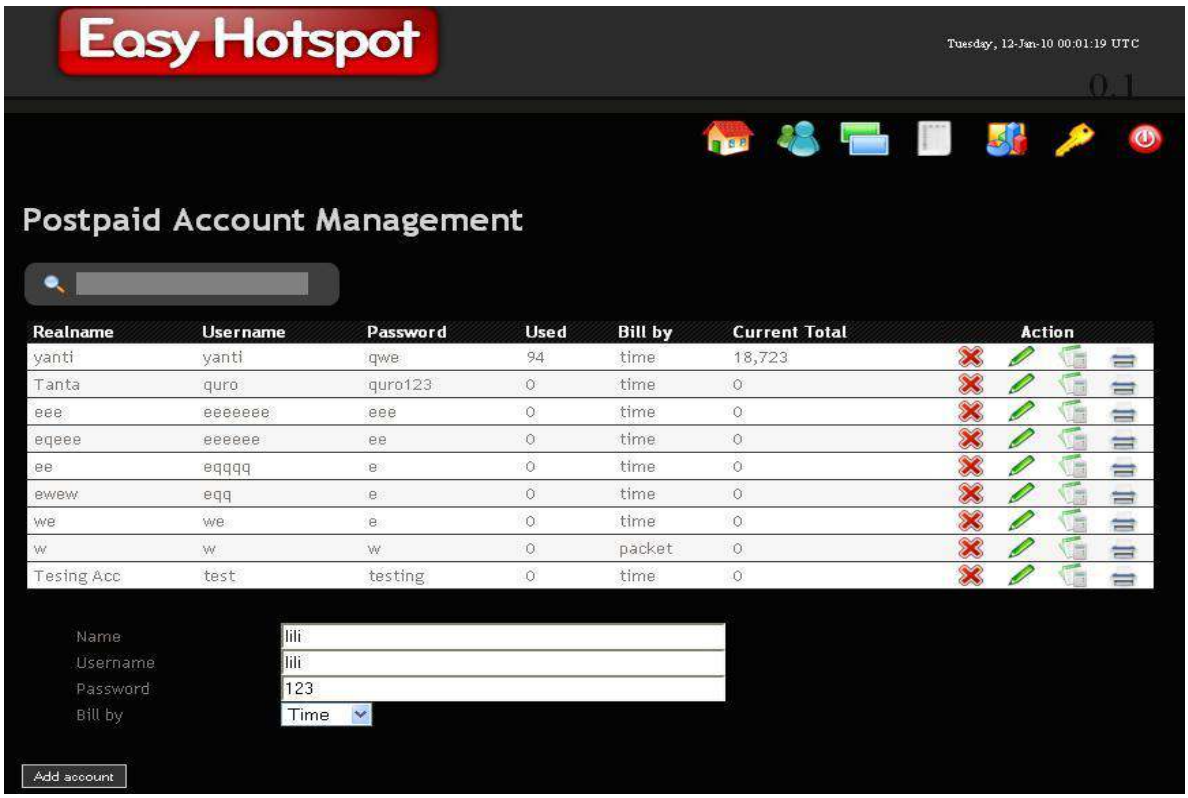
Change password



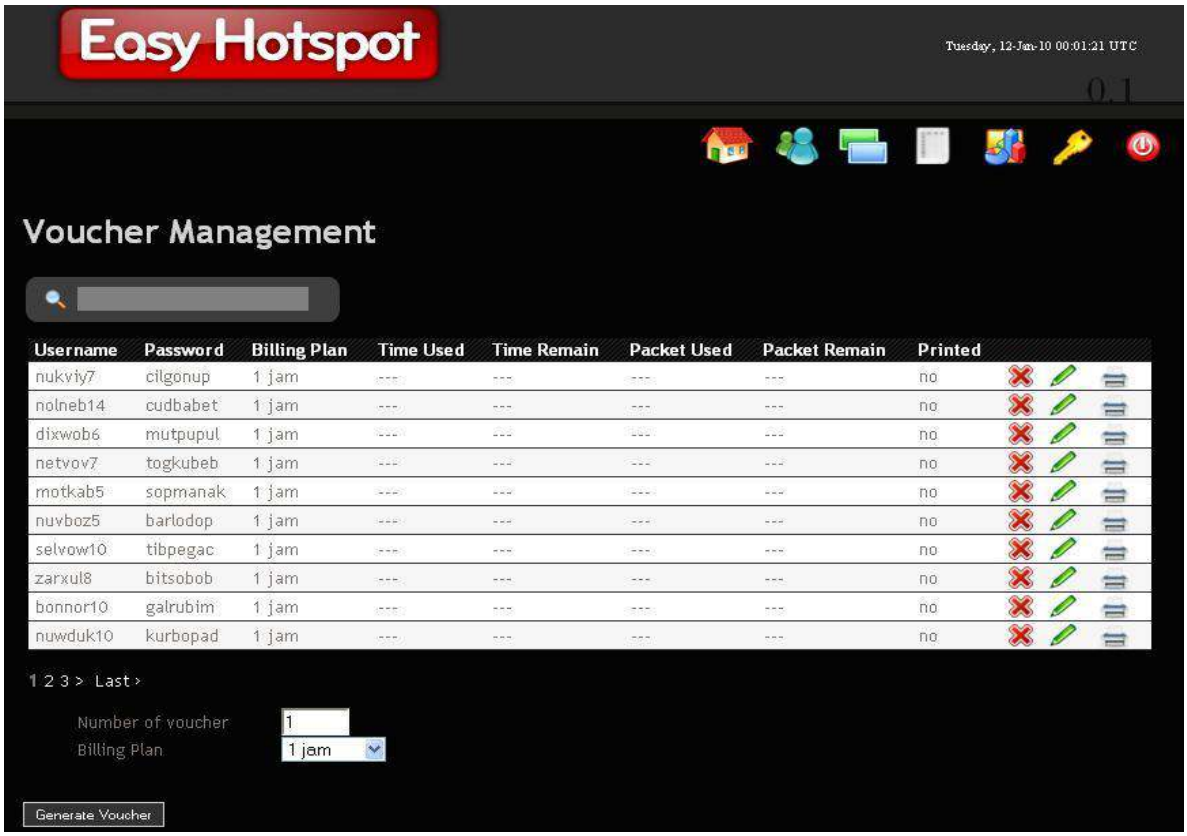
Login kasir

Menu kasir

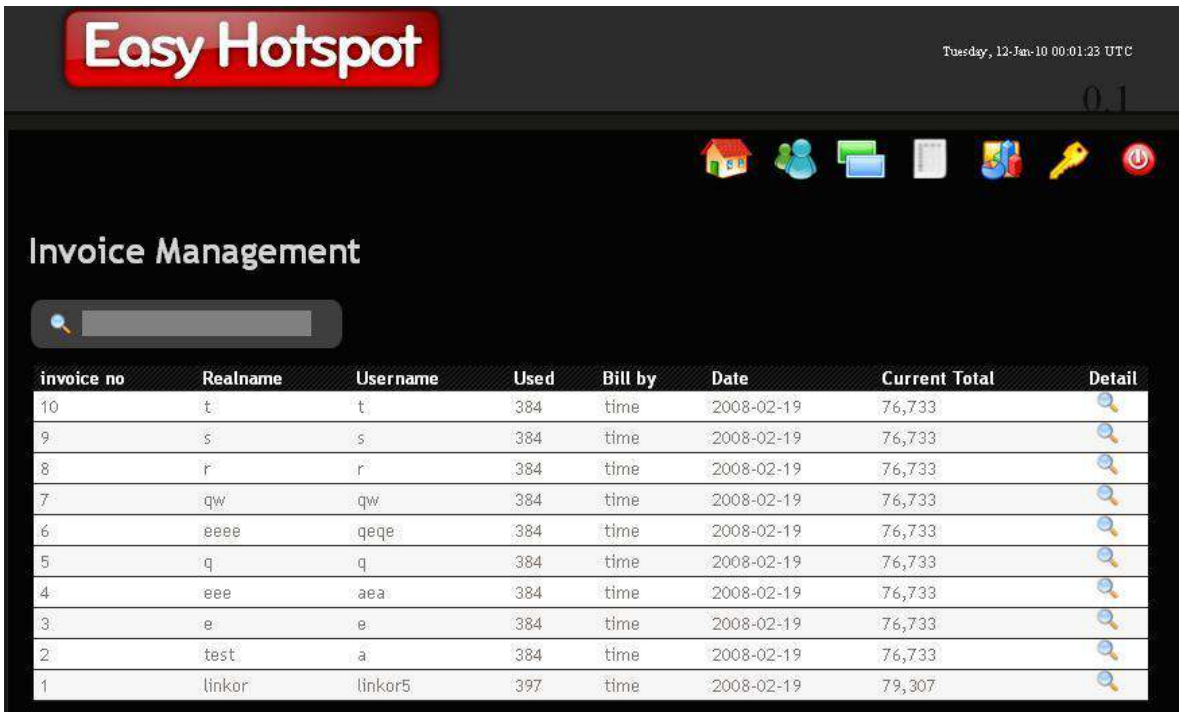
Postpaid account kasir



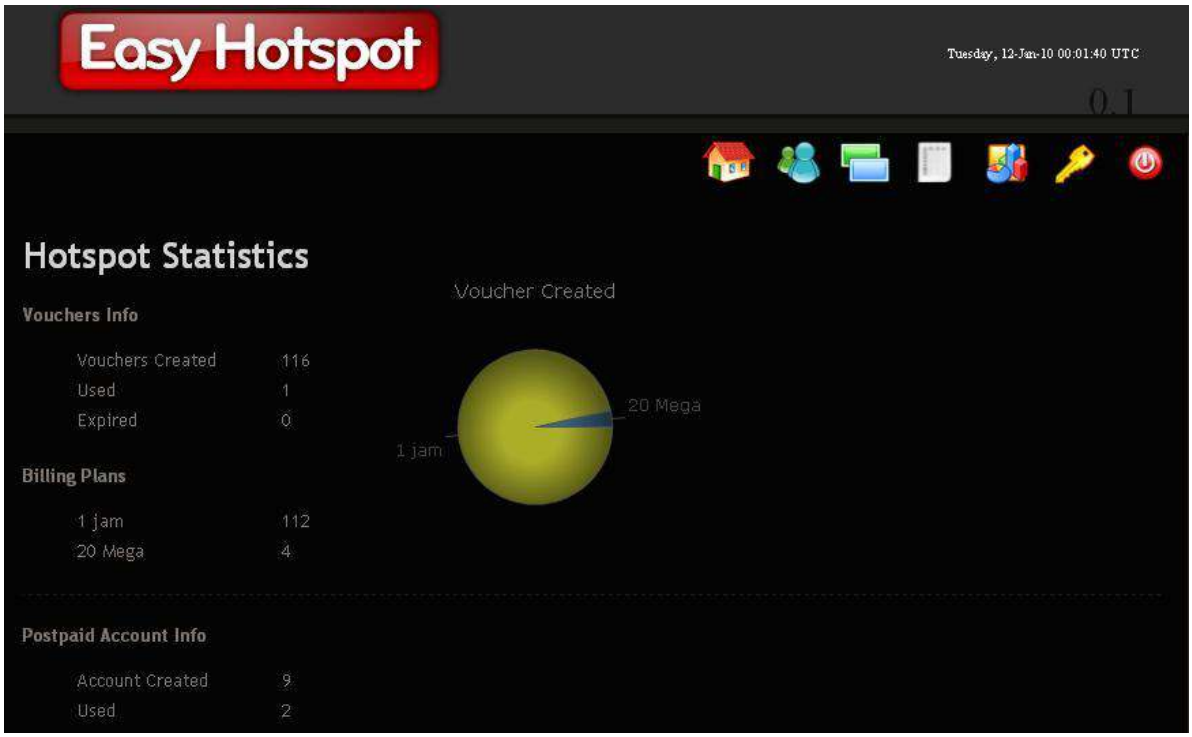
Voucher kasir



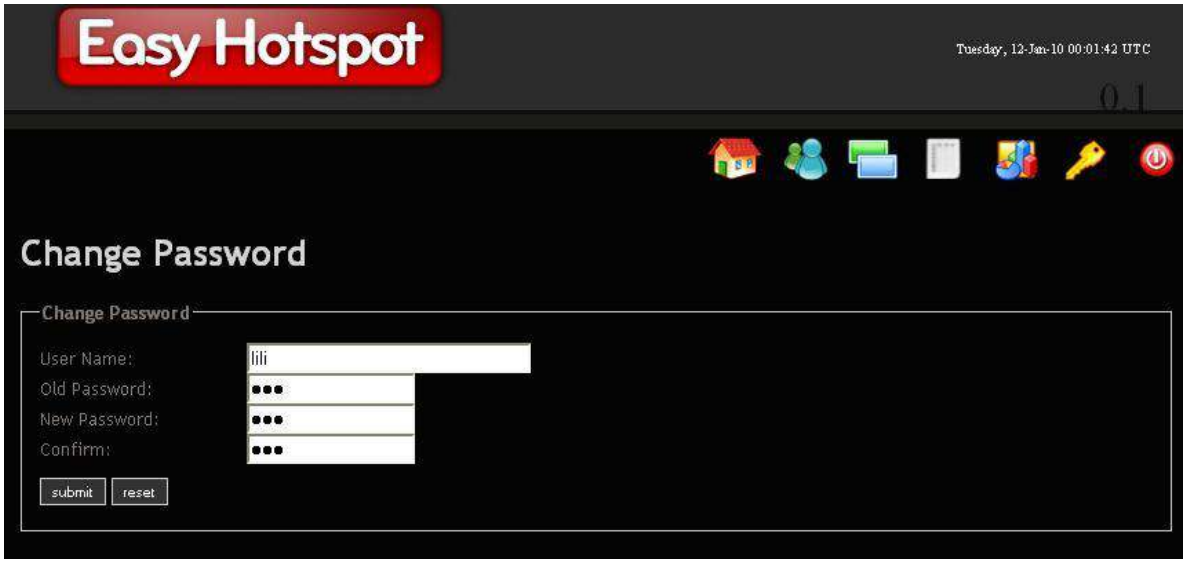
Pembuatan Invoice pada kasir



Hotspot statistic kasir

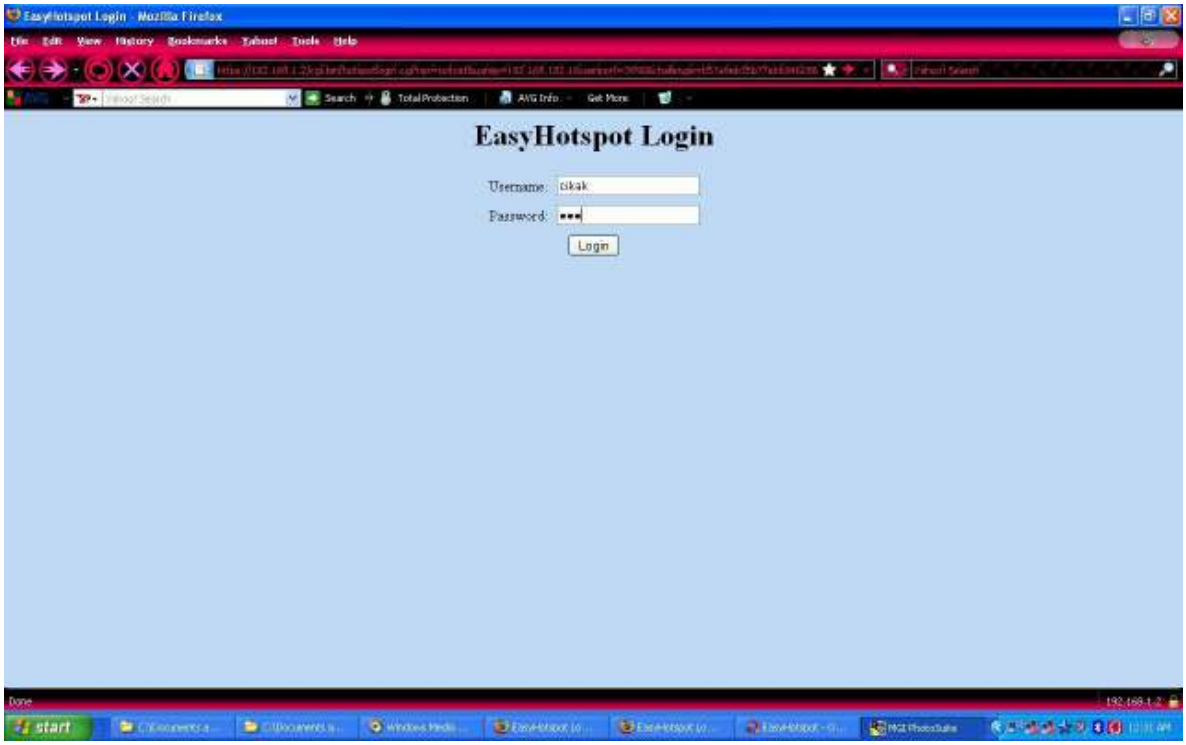


Change password kasir

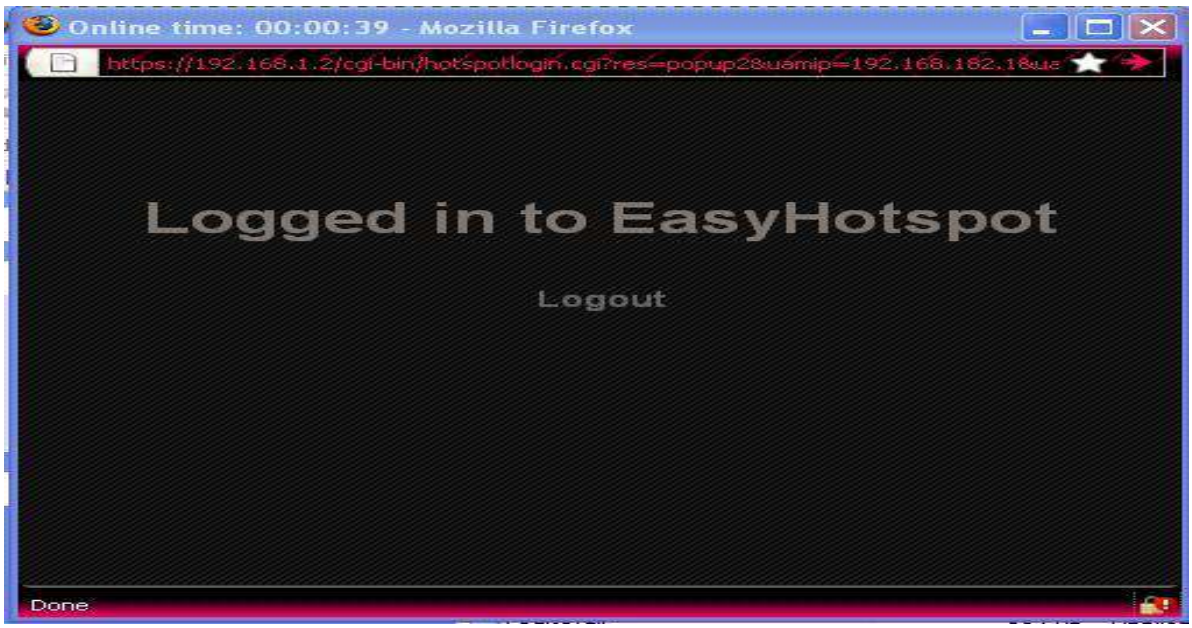


Untuk mengetahui kemampuan easyhotspot, dapat dilakukan sebuah percobaan sederhana menggunakan software sniffer yang bernama cain and able.

Login easyhotspot



Logout easyhotspot



Karena easyhotspot menggunakan protokol https sehingga menyebabkan aktifitas sniffing username dan password menjadi tidak berguna(username dan password yang tertangkap tidak sesuai dengan aslinya).