

**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

HALAMAN JUDUL	i
LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN.....	iii
KATA PENGANTAR.....	iv
ABSTRAKSI.....	v
ABSTRACT	vi
DAFTAR ISI	vii
DAFTAR GAMBAR.....	ix
DAFTAR TABEL	ix
Bab 1 Pendahuluan	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	1
1.3 Batasan Masalah	1
1.4 Tujuan Penelitian.....	2
1.5 Sistematika Penulisan	2
Bab 2 Landasan teori.....	3
2.1 Definisi Captive Portal	3
2.2 Definisi Router	4
2.3 Definisi Open source	5
2.4 Topologi Jaringan	6
2.4.1 Topologi Bus	6
2.4.2 Topologi Star.....	7
2.4.3 Topologi Ring	9
2.4.4 Topologi Mesh	10
2.4.5 Topologi Pohon (Tree).....	11
2.4.6 Topologi Hybrid (Campuran).....	12

Bab 3	Pemilihan dan Perancangan Pengujian Captive Portal.....	13
3.1	Proses Pemilihan	13
3.2	Jenis dan Software Captive Portal.....	14
3.2.1	Monowall	18
3.2.2	Pfsense.....	21
3.2.3	Easy Hotspot	24
3.3	Perancangan Pengujian.....	26
3.3.1	Skema Jaringan	26
3.3.2	Lingkungan Pengujian.....	27
3.3.3	Kriteria Evaluasi	28
Bab 4	Implementasi dan Pembahasan	31
4.1	Konfigurasi PC Router	31
4.2	Implementasi Monowall.....	31
4.3	Implementasi Pfsense	34
4.4	Implementasi Easy Hotspot.....	37
4.5	Perbandingan Monowall, Pfsense dan Easy Hotspot	39
Bab 5	Kesimpulan dan Saran.....	42
5.1	Kesimpulan.....	42
5.2	Saran	43
DAFTAR PUSTAKA.....		44
LAMPIRAN PROSES IMPLEMENTASI		45
1.1	Monowall.....	45
1.2	Pfsense	73
1.3	Easy Hotspot.....	107

DAFTAR GAMBAR

Gambar 2.1 Definisi Captive Portal	3
Gambar 2.4.1 Topologi Bus	6
Gambar 2.4.2 Topologi Star	7
Gambar 2.4.3 Topologi Ring	9
Gambar 2.4.4 Topologi Mesh	10
Gambar 2.4.5 Topologi Pohon	11
Gambar 2.4.6 Topologi Hybrid	12
Gambar 3.2.1 Tampilan webGUI Monowall	18
Gambar 3.2.2 Tampilan webGUI Pfsense	22
Gambar 3.2.3 Tampilan Menu Admin Easy Hotspot	25
Gambar 3.3.1 Topologi Jaringan Star	26
Gambar 4.2 Topologi Jaringan Monowall	31
Gambar 4.3 Topologi Jaringan Pfsense	34
Gambar 4.4 Topologi Jaringan Easy Hotspot	37

DAFTAR TABEL

Tabel 3.2.1 Deskripsi Software Captive Portal	15
Tabel 3.3.2.1 Spesifikasi PC Server Monowall	27
Tabel 3.3.2.2 Spesifikasi PC Server Pfsense	27
Tabel 3.3.2.3 Spesifikasi PC Server Easy Hotspot	27
Tabel 3.3.2.4 Spesifikasi PC Client	27
Tabel 3.3.2.5 Spesifikasi PC Router	28
Tabel 3.3.2.6 Komponen Pendukung	28
Tabel 3.3.3.1 Fleksibilitas	29
Tabel 3.3.3.2 Support	30

Tabel 3.3.3.3 Kesenambungan.....	30
Tabel 4.2.1 Evaluasi Monowall	33
Tabel 4.3.1 Evaluasi Pfsense.....	36
Tabel 4.4.1 Evaluasi Easy Hotspot.....	38
Tabel 5.1.1 Kesimpulan	39

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.

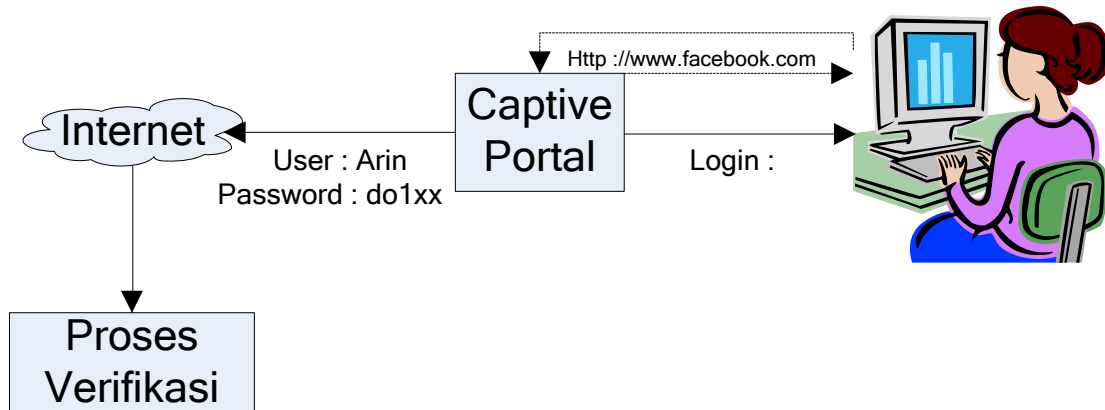
Bab 3 Pemilihan dan Perancangan Pengujian Captive Portal berisi tentang urutan proses/langkah dalam melakukan pemilihan software captive portal, jenis dan software captive portal, software-software yang digunakan dalam proses perbandingan, serta perancangan pengujian software captive portal yang meliputi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

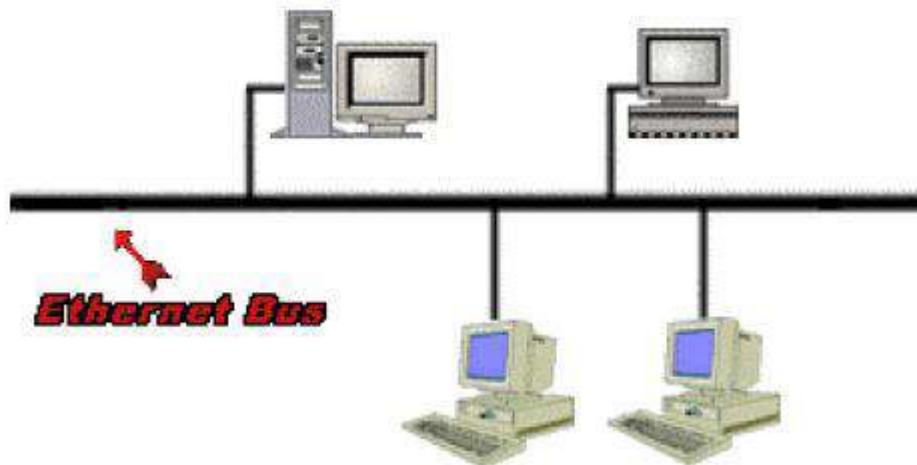
Open source software adalah istilah yang digunakan untuk software yang membuka/membebasikan source codenya untuk dilihat oleh orang lain, dan membiarkan orang lain mengetahui cara kerja serta memperbaiki kelemahan-kelemahan yang ada pada software tersebut. Syarat-syarat distribusi open source software 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 digabungkan dengan topologi star untuk menghubungkan dengan client atau node).

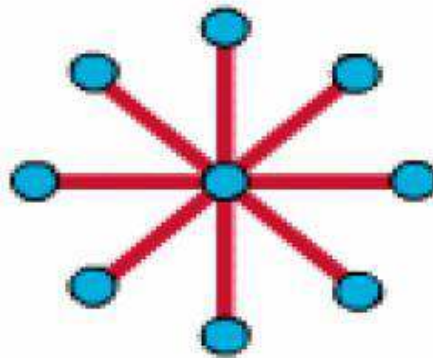
Keuntungan:

- 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 ke semua 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. Terdapat keuntungan dan kerugian dari tipe ini yaitu:

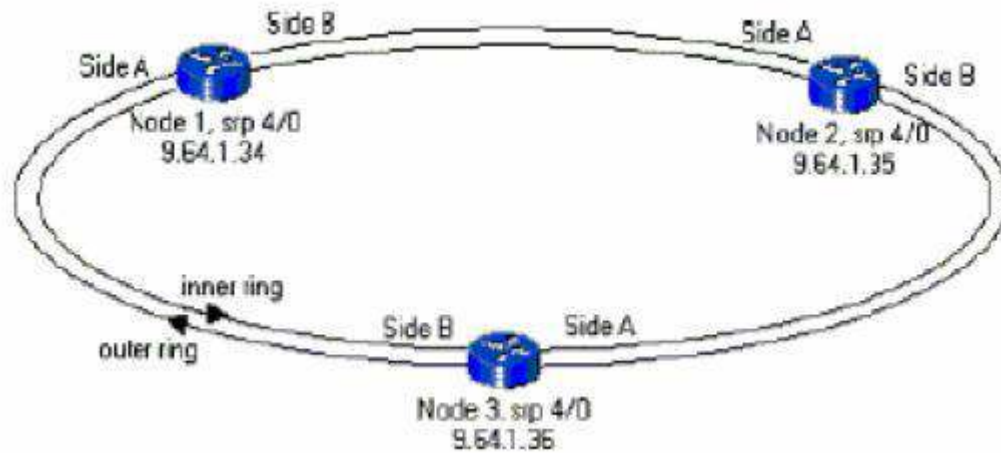
Keuntungan:

- Paling fleksibel
- Pemasangan/perubahan stasiun sangat mudah dan tidak mengganggu bagian jaringan lain.
- Kontrol terpusat
- 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 ke semua 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).

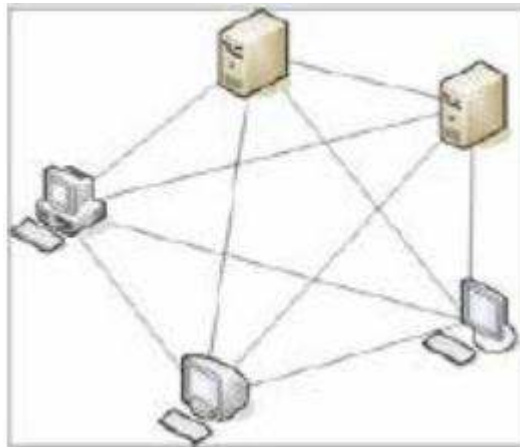
Keuntungan:

- Hemat kabel

Kerugian:

- Peka kesalahan
- Pengembangan jaringan lebih kaku

2.4.4 Topologi Mesh



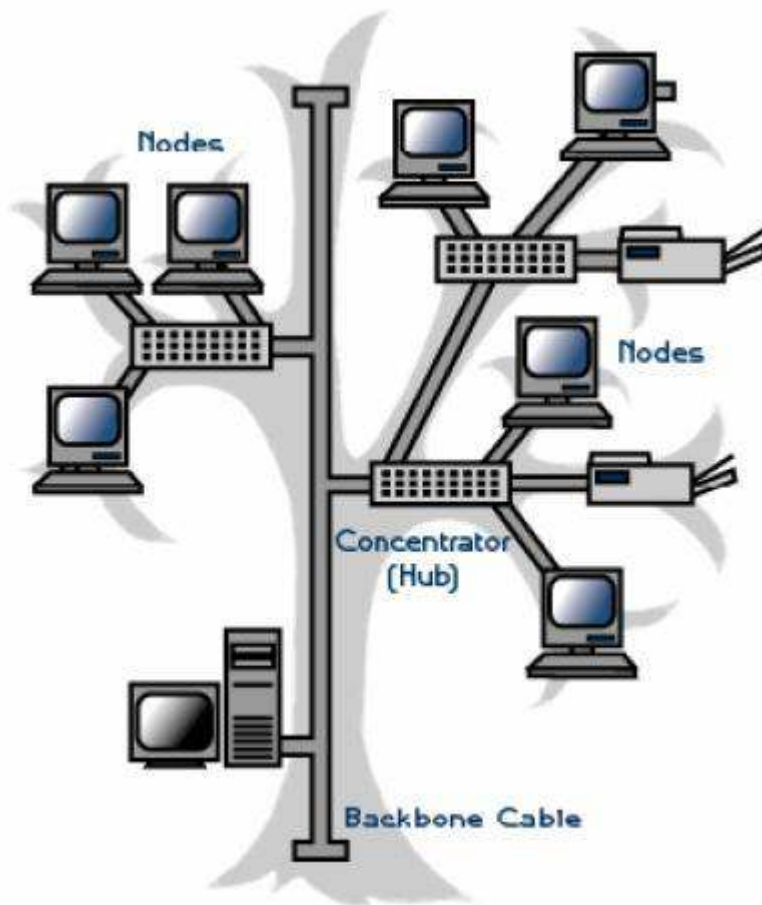
Gambar 2.4.4 Topologi Mesh

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)

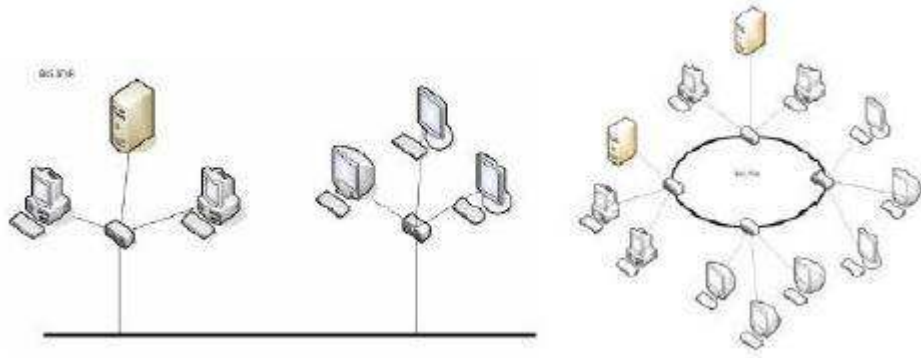


Gambar 2.4.5 Topologi Pohon

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 karakteristik 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® mengizinkan 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.



The screenshot displays the Monowall webGUI Configuration interface. The top navigation bar includes the Monowall logo, the title "webGUI Configuration", and the URL "m0n0wall.local". A left sidebar lists various configuration categories: System, Interfaces, Firewall, Services, VPN, and Status. The main content area features a large Monowall logo and a "System information" table.

System information	
Name	m0n0wall.local
Version	1.3b15 built on Sat Oct 11 18:48:17 CEST 2008
Platform	Generic PC (CD-ROM)
Uptime	00:02
Last config change	Sat Jan 15 12:52:41 UTC 2005
CPU usage	view graph
Memory usage	<input type="text" value="8%"/>
Notes	<div style="border: 1px solid #ccc; height: 80px;"></div> <input type="button" value="Save"/>

At the bottom of the page, a footer reads: "m0n0wall® is © 2002-2008 by Manuel Kasper. All rights reserved. [view license]"

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 informasi yang dibutuhkan bagi pengelolanya.
15. Traffic shaper, pembagian atau pengaturan bandwidth 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.

The screenshot shows the pfSense webConfigurator interface. On the left is a navigation menu with categories: System, Interfaces, Firewall, and Services. The main content area is titled 'System Overview' and contains a 'System information' table and resource usage bars.

System information	
Name	maria.atnoba.com
Version	1.2.3-RC1 built on Wed Apr 22 15:26:34 EDT 2009
Platform	pfSense
Uptime	06:13
State table size	25/10000 Show states
MBUF usage	135/390
CPU usage	<div style="width: 0%;"></div> 0%
Memory usage	<div style="width: 47%;"></div> 47%
SWAP usage	<div style="width: 0%;"></div> 0%
Disk usage	<div style="width: 1%;"></div> 1%

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 bandwidth 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 melalui 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:

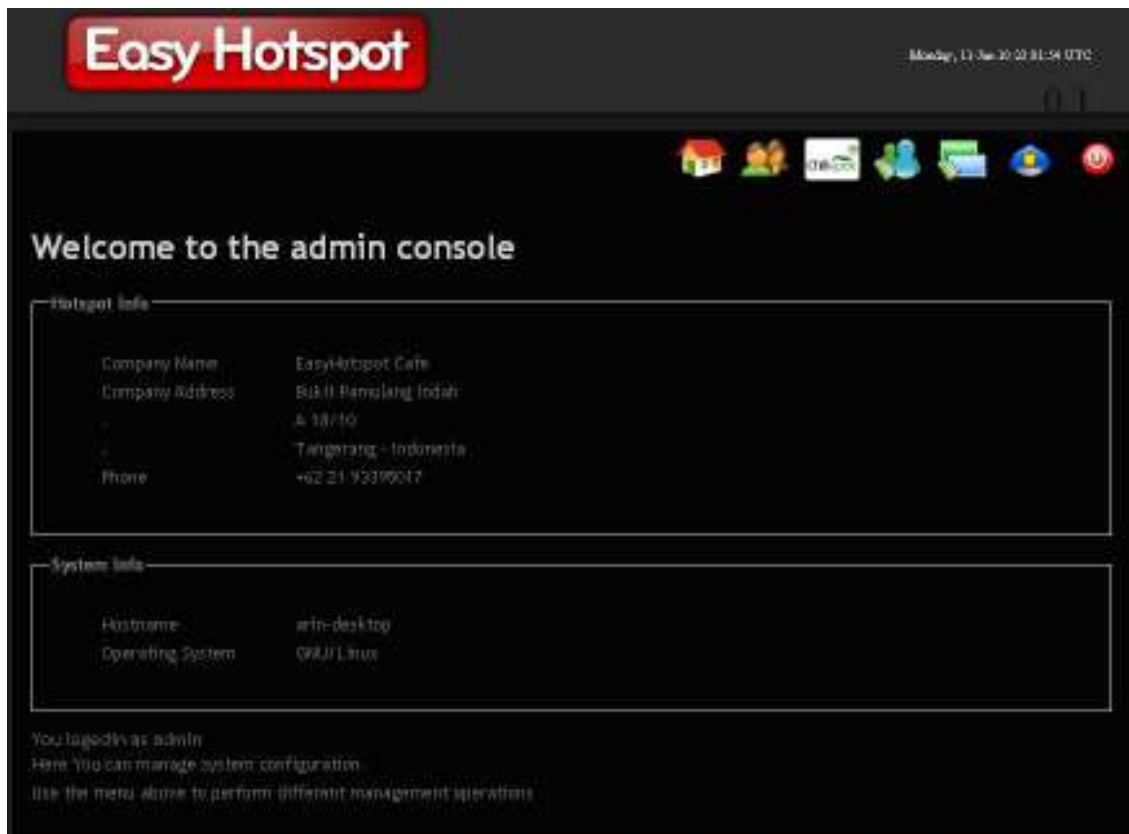
1. **MySql**: Sarana penyimpanan data-data dan informasi-informasi
2. **FreeRadius**: Untuk membangun Radius Server, yaitu merupakan sebuah aplikasi yang memungkinkan keamanan jaringan wireless untuk melakukan authentication, authorize, dan accounting. Selain itu dapat pula untuk mengontrol para pengguna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

Easy hotspot memiliki pengaturan sistem hotspot dengan menggunakan web interface yang mengatur semua hal yang berhubungan dengan administrasi pemakaian dan aktivitas penagihan. Easy hotspot 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).

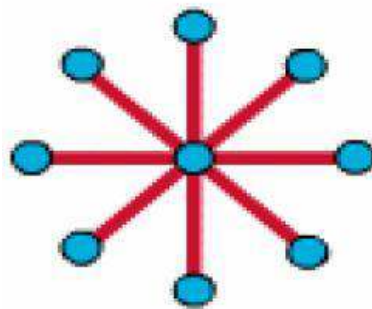
3. Pengaturan billing, prepaid (voucher) dan postpaid (biaya akan dihitung setelah pengguna selesai mengakses internet)
4. Statistik, untuk mengetahui pengguna yang aktif dan pengguna harian.
5. Konfigurasi, untuk mengganti password admin dan pengaturan halaman yang dapat diakses, serta secret key.

3.3 Perancangan Pengujian

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

3.3.1 Skema Jaringan

Captive portal dapat diterapkan 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 penggunaannya 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 pemrograman, 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 pemrograman	:	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

- Kesenambungan
Kesenambungan dijabarkan menjadi status pengembangan(menjelaskan mengenai proses pengembangan software).

Tabel 3.3.3.3 Kesenambungan

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 pengarahannya pada nameservernya perintahnya adalah **#nano /etc/network/interfaces :**

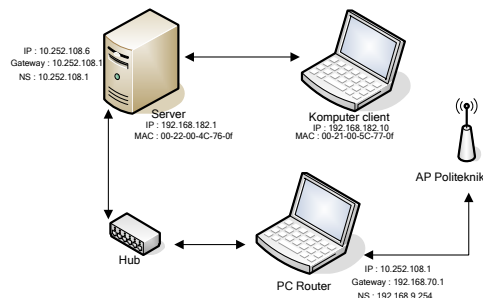
```
auto lo
iface lo inet loopback

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 menghapus 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. Masukkan alamat IP static yang dipergunakan beserta IP gateway. Melakukan pengaturan pada menu general setup, seperti pemberian nama server yang dibangun, DNS, pemilihan port http/https.
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.

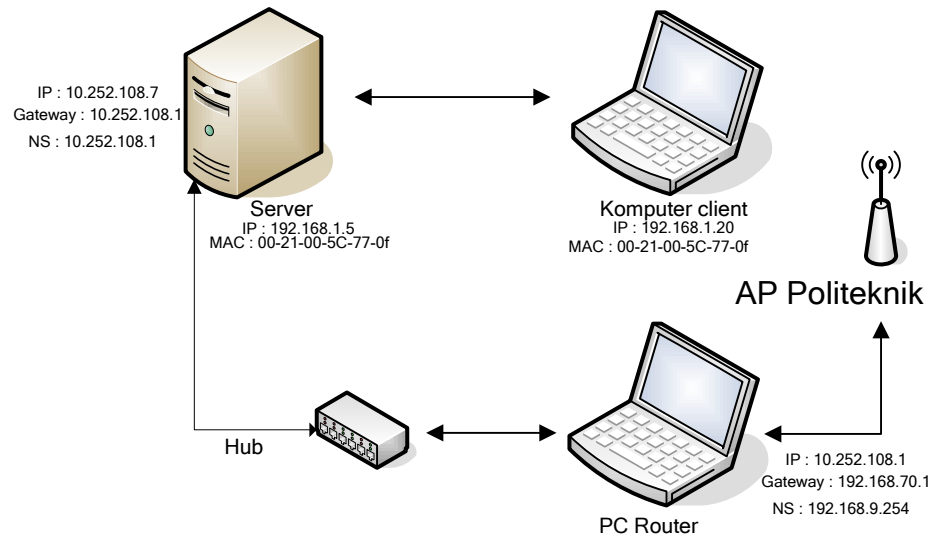
Bahasa pemrograman yang digunakan adalah PHP yang digabungkan dengan unsur-unsur lainnya. Selain dapat memanfaatkan software tersebut secara gratis, dapat melakukan perubahan atau pembaharuan sesuai dengan kebutuhan yang diinginkan. Pengguna juga dapat menikmati layanan komunitas yang berfungsi sebagai 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 pemrograman	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

berdasarkan voucher	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 dilihat pada lampiran).

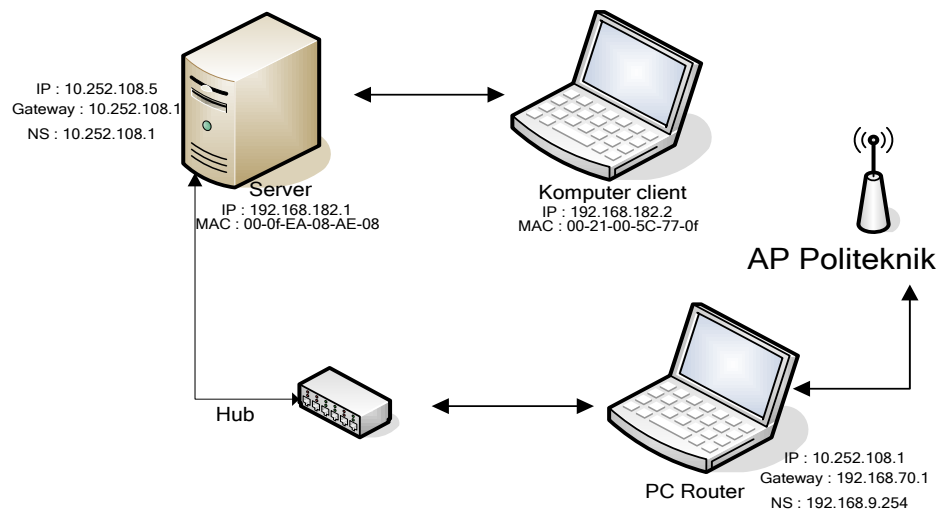
Pfsense merupakan firewall, penggunaannya tidak ditujukan untuk embedded PC. Dapat difungsikan untuk pengaturan internet connection sharing. Memiliki beberapa macam versi yang dapat digunakan sesuai dengan pemakaian pengguna. Penggunaannya memberikan support pada satu macam bahasa yakni bahasa inggris. 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 pemrograman yang digunakan adalah PHP yang digabungkan dengan unsur-unsur lainnya. Pengguna selain dapat memanfaatkan software tersebut secara gratis, dapat pula melakukan perubahan 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 pemrograman	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 mailing 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 perubahan 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. Penggunaannya cukup mudah yakni

melalui webGUI. Skalabilitasnya cukup baik. Memiliki pengaturan firewall. Bahasa pemrograman 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 memanfaatkannya 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 pemrograman	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, SATA tidak support, wireless card dan Ethernet card yang dikenali terbatas	Support penggunaan berbagai macam wireless card terutama atheros, komputer dengan spesifikasi yang besar	komputer dengan spesifikasi yang besar
Bahasa pemrograman	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, mailing list, IRC channel	Forum, mailing 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 Penggunaan voucher tidak terpengaruh pada koneksi mempergunakan port https digunakan pada jaringan yang besar dan kecil memiliki pengaturan traffic shaper	difungsikan sebagai router dan pengaturan internet terdapat fitur-fitur tambahan terdapat antivirus dan konfigurasi untuk multiple uplink mempergunakan port https digunakan pada jaringan yang besar dan kecil memiliki pengaturan traffic shaper	difungsikan untuk mengatur billing hotspot dapat dilakukan instalasi untuk aplikasi lain mempergunakan port https
Kekurangan	dalam pembuatan voucher, terjadi voucher ganda tidak difungsikan untuk pengaturan billing hotspot	tidak difungsikan untuk pengaturan billing hotspot	digunakan pada jaringan yang kecil 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 bandwidth 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 perbandingan software captive portal yang dapat dipergunakan sebagai acuan dalam pemilihan sebuah software captive portal.
3. Untuk melakukan perbandingan 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 menanggulangi 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.

```
*** This is m0n0wall, version 1.3b15
    built on Sat Oct 11 18:48:17 CEST 2008 for generic-pc-cdrom
    Copyright (C) 2002-2008 by Manuel Kasper. All rights reserved.
    Visit http://m0n0.ch/wall for updates.

    LAN IP address: 192.168.1.1

    Port configuration:

    LAN    -> sis0
    WAN    -> sis1

m0n0wall console setup
*****
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host
7) Install on Hard Drive

Enter a number: 1
```

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 perubahan 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 digunakan 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.

```

7) Install on Hard Drive
Enter a number: 1
Valid interfaces are:
pcn0  08:00:27:b1:93:d2  (up)  AMD PCnet/PCI 10/100BaseTX ← interface yang dikenali
pcn1  08:00:27:2b:24:5b  (up)  AMD PCnet/PCI 10/100BaseTX
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):

```

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 menentukan 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 menampilkan 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).

```
m0n0wall console setup
*****
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host
7) Install on Hard Drive

Enter a number: 2

Enter the new LAN IP address: 192.168.182.1

Subnet masks are entered as bit counts (as in CIDR notation) in m0n0wall.
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: 192.168.182.2
Enter the end address of the client address range: 192.168.182.10
```

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 pertanyaan 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.

```
7) Install on Hard Drive
Enter a number: 2
Enter the new LAN IP address: 192.168.182.1
Subnet masks are entered as bit counts (as in CIDR notation) in m0n0wall.
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: 192.168.182.2
Enter the end address of the client address range: 192.168.182.10
The LAN IP address has been set to 192.168.182.1/24.
You can now access the webGUI by opening the following URL
in your browser:
http://192.168.182.1/
Press ENTER to continue.
```

kemudian akan muncul pernyataan bahwa IP address 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)

The screenshot displays the 'webGUI Configuration' page for 'Interfaces: WAN'. The left sidebar contains a navigation menu with categories like System, Interfaces, Firewall, Services, VPN, and Status. The main content area is divided into several configuration sections:

- General configuration:** Includes a 'MAC address' field with a descriptive note: 'This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.'
- Static IP configuration:** Includes an 'IP address' field (10.252.108.6) and a subnet mask dropdown (28), and a 'Gateway' field (10.252.108.1).
- DHCP client configuration:** Includes a 'Hostname' field with a note: 'The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).'
- PPPoE configuration:** Includes 'Username', 'Password', and 'Service name' fields. A hint for 'Service name' states: 'Hint: this field can usually be left empty'. It also includes an 'MTU' field with a note: 'Usually, the maximum MTU value of 1492 bytes (which is used by default) works fine, but if you have problems with some sites not loading properly, you can try a smaller value (e.g. 1400) here.'
- PPTP configuration:** Includes a 'Username' field.

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.

System

- General setup
- Static routes
- Firmware
- Advanced
- User manager

Interfaces (assign)

- LAN
- WAN

Firewall

- Rules
- NAT
- Traffic shaper
- Aliases

Services

- DNS forwarder
- Dynamic DNS
- DHCP server
- DHCP relay
- SNMP
- Proxy ARP
- Captive portal
- Wake on LAN

VPN

- IPsec
- PPTP

Status

- System
- Interfaces
- Traffic graph
- Wireless
- Captive portal

► **Diagnostics**

Services: Captive portal

Captive Portal | Pass-through MAC | Allowed IP addresses | Users | Vouchers | File Manager

Enable captive portal

Interface	LAN Choose which interface to run the captive portal on.
Maximum concurrent connections	<input type="text"/> per client IP address (0 = no limit) <input type="text"/> total This setting limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many users can load the portal page or authenticate at the same time! Default is 4 connections per client IP address, with a total maximum of 16 connections.
Idle timeout	<input type="text"/> minutes Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.
Hard timeout	60 minutes Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).
Logout popup window	<input type="checkbox"/> Enable logout popup window If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.
Redirection URL	<input type="text"/> If you provide a URL here, clients will be redirected to that URL instead of the one they initially tried to access after they've authenticated.
Concurrent user logins	<input type="checkbox"/> Disable concurrent logins If this option is set, only the most recent login per username will be active. Subsequent logins will cause machines previously logged in with the same username to be disconnected.
MAC filtering	<input type="checkbox"/> Disable MAC filtering If this option is set, no attempts will be made to ensure that the MAC address of clients stays the same while they're logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between m0n0wall and the clients).
Per-user bandwidth restriction	<input type="checkbox"/> Enable per-user bandwidth restriction Default download <input type="text"/> Kbit/s Default upload <input type="text"/> Kbit/s

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.

System

- General setup
- Static routes
- Firmware
- Advanced
- User manager

Interfaces (assign)

- LAN
- WAN

Firewall

- Rules
- NAT
- Traffic shaper
- Aliases

Services

- DNS forwarder
- Dynamic DNS
- DHCP server
- DHCP relay
- SNMP
- Proxy ARP
- Captive portal
- Wake on LAN

VPN

- IPsec
- PPTP

Status

- System
- Interfaces
- Traffic graph
- Wireless
- Captive portal

▶ **Diagnostics**

Services: Captive portal: Vouchers

Captive Portal
Pass-through MAC
Allowed IP addresses
Users
Vouchers
File Manager

Enable Vouchers

Membuat voucher

Voucher Rolls	Roll#	Minutes/Ticket	# of Tickets	Comment
<p>Create, generate and activate Rolls with Vouchers that allow access through the captive portal for the configured time. Once a voucher is activated, its clock is started and runs uninterrupted until it expires. During that time, the voucher can be re-used from the same or a different computer. If the voucher is used again from another computer, the previous session is stopped.</p>				
Voucher public key	<pre>-----BEGIN PUBLIC KEY----- MCQwDQYJKoZIhvcNAQEBBQADEwAwEAIJAL2dCqa0+0U/AgMBAAE= -----END PUBLIC KEY-----</pre> <p>Paste an RSA public key (64 Bit or smaller) in PEM format here. This key is used to decrypt vouchers.</p>			
Voucher private key	<pre>-----BEGIN RSA PRIVATE KEY----- MD0CAQACCCQ9nQgm1vj1fwIDAQABAgghjL1aeCNY=QIFAM/U0ycCBQDY3dnpAgQe Hp4TAgRe0BypAgQumJjj -----END RSA PRIVATE KEY-----</pre> <p>Paste an RSA private key (64 Bit or smaller) in PEM format here. This key is only used to generate encrypted vouchers and doesn't need to be available if the vouchers have been generated offline.</p>			
Character set	<input style="width: 100%;" type="text" value="2345678abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"/> <p>Tickets are generated with the specified character set. It should contain printable characters (numbers, lower case and upper case letters) that are hard to confuse with others. Avoid e.g. 0/O and l/1.</p>			
# of Roll Bits	<input style="width: 50%;" type="text" value="16"/> <p>Reserves a range in each voucher to store the Roll# it belongs to. Allowed range: 1..31. Sum of Roll+Ticket+Checksum bits must be one Bit less than the RSA key size.</p>			
# of Ticket Bits	<input style="width: 50%;" type="text" value="10"/> <p>Reserves a range in each voucher to store the Ticket# it belongs to. Allowed range: 1..16. Using 16 bits allows a roll to have up to 65535 vouchers. A bit array, stored in RAM and in the config, is used to mark if a voucher has been used. A bit array for 65535 vouchers requires 8 KB of storage.</p>			
# of Checksum Bits	<input style="width: 50%;" type="text" value="5"/> <p>Reserves a range in each voucher to store a simple checksum over Roll# and Ticket#. Allowed range is 0..31.</p>			

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

The screenshot shows the m0n0wall webGUI Configuration interface. The left sidebar contains a navigation menu with categories like System, Interfaces, Firewall, Services, VPN, and Status. The main content area is titled 'Services: Captive portal: Edit Voucher Rolls'. It features a form with the following fields:

- Roll#:** 1 (with a note: 'Enter the Roll# (0..65535) found on top of the generated/printed vouchers.')
- Minutes per Ticket:** 3 (with a note: 'Defines the time in minutes that a user is allowed access. The clock starts ticking the first time a voucher is used for authentication.')
- Count:** 5 (with a note: 'Enter the number of vouchers (1..1023) found on top of the generated/printed vouchers. WARNING: Changing this number for an existing Roll will mark all vouchers as unused again.')
- Comment:** 'her berjumlah 5 buah dengan lama periode aktifasi selama 3 menit' (with a note: 'Can be used to further identify this roll. Ignored by the system.')

A 'Save' button is located below the form. At the bottom of the page, a footer reads: 'm0n0wall® is © 2002-2008 by Manuel Kasper. All rights reserved. [view license]'.

Proses generate voucher(menampilkan voucher yang telah dibuat)

The screenshot shows the m0n0wall webGUI Configuration interface for 'Services: Captive portal: Vouchers'. The left sidebar is the same as in the previous screenshot. The main content area has a sub-header 'Services: Captive portal: Vouchers' and a navigation bar with tabs: 'Captive Portal', 'Pass-through MAC', 'Allowed IP addresses', 'Users', 'Vouchers', and 'File Manager'. The 'Vouchers' tab is active, and a sub-tab 'generate voucher yang telah dibuat' is visible. A checkbox 'Enable Vouchers' is checked. Below this is a table of Voucher Rolls:

Voucher Rolls	Roll#	Minutes/Ticket	# of Tickets	Comment
	1	3	5	voucher berjumlah 5 buah dengan lama periode aktifasi selama 3 menit

Below the table, there are sections for 'Voucher public key' and 'Voucher private key', each containing a PEM-formatted key. The 'Character set' field is set to '2345678abcdehijklmnpqrstuvwxyzABCDEFGHIJKLMNPQRSTUVWXYZ'. The '# of Roll Bits' is set to 16, and the '# of Ticket Bits' is set to 10. A note at the bottom states: 'Reserves a range in each voucher to store the Ticket# it belongs to. Allowed range: 1..16. Using 16 bits allows a roll to have up to 65535 vouchers. A bit array, stored in RAM and in the config, is used to mark if a voucher has been used. A bit array for 65535 vouchers requires 8 KB of storage.'

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 2345678abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNPQRSTUVWXYZ										
#										
Pb8GEbSscu	}	voucher								
Lii3EWnw4Ym										
QisvyPK4tqB										

Untuk melakukan uji coba pada voucher yang telah dibuat, langkah pertama yang dilakukan adalah membuka web browser kemudian menyetikkan 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 memasukkan nomor voucher pada kolom voucher yang telah disediakan.

MONOSPOT

Silakan masukan voucher anda untuk login !

Voucher:

Menyediakan koneksi internet hotspot dengan sistem:

1. Voucher Rp. 5.000 / 2 jam
2. Voucher Rp. 10.000 / 4 jam.

Hubungi **085264699959** untuk keterangan lebih lanjut.

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

Authentication error

Username and/or password invalid.

[Go back](#)

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

System

- General setup
- Static routes
- Firmware
- Advanced
- User manager

Interfaces (assign)

- LAN
- WAN

Firewall

- Rules
- NAT
- Traffic shaper
- Aliases

Services

- DNS forwarder
- Dynamic DNS
- DHCP server
- DHCP relay
- SNMP
- Proxy ARP
- Captive portal
- Wake on LAN

VPN

- IPsec
- PPTP

Status

- System
- Interfaces
- Traffic graph
- Wireless
- Captive portal

▶ **Diagnostics**

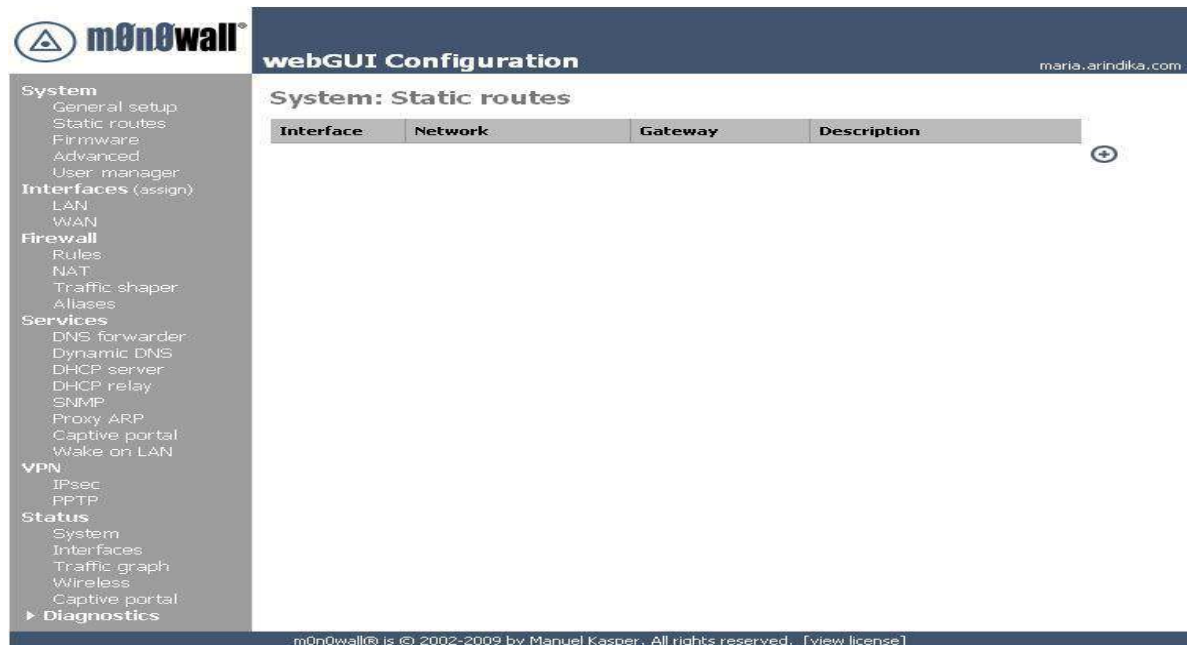
Firewall: Rules: Edit

Action	Reject <input type="button" value="v"/> Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	LAN <input type="button" value="v"/> Choose on which interface packets must come in to match this rule.
Protocol	TCP <input type="button" value="v"/> Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.
ICMP type	any <input type="button" value="v"/> If you selected ICMP for the protocol above, you may specify an ICMP type here.
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: any <input type="button" value="v"/> Address: <input type="text" value=""/> / 31 <input type="button" value="v"/>
Source port range	from: any <input type="button" value="v"/> <input type="text" value=""/> to: any <input type="button" value="v"/> <input type="text" value=""/> Specify the port or port range for the source of the packet for this rule. This is usually not equal to the destination port range (and is often "any"). Hint: you can leave the 'to' field empty if you only want to filter a single port
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: Single host or alias <input type="button" value="v"/> Address: 119.2.43.84 <input type="text" value=""/> / 31 <input type="button" value="v"/>
Destination port range	from: any <input type="button" value="v"/> <input type="text" value=""/> to: any <input type="button" value="v"/> <input type="text" value=""/> Specify the port or port range for the destination of the packet for this rule.

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

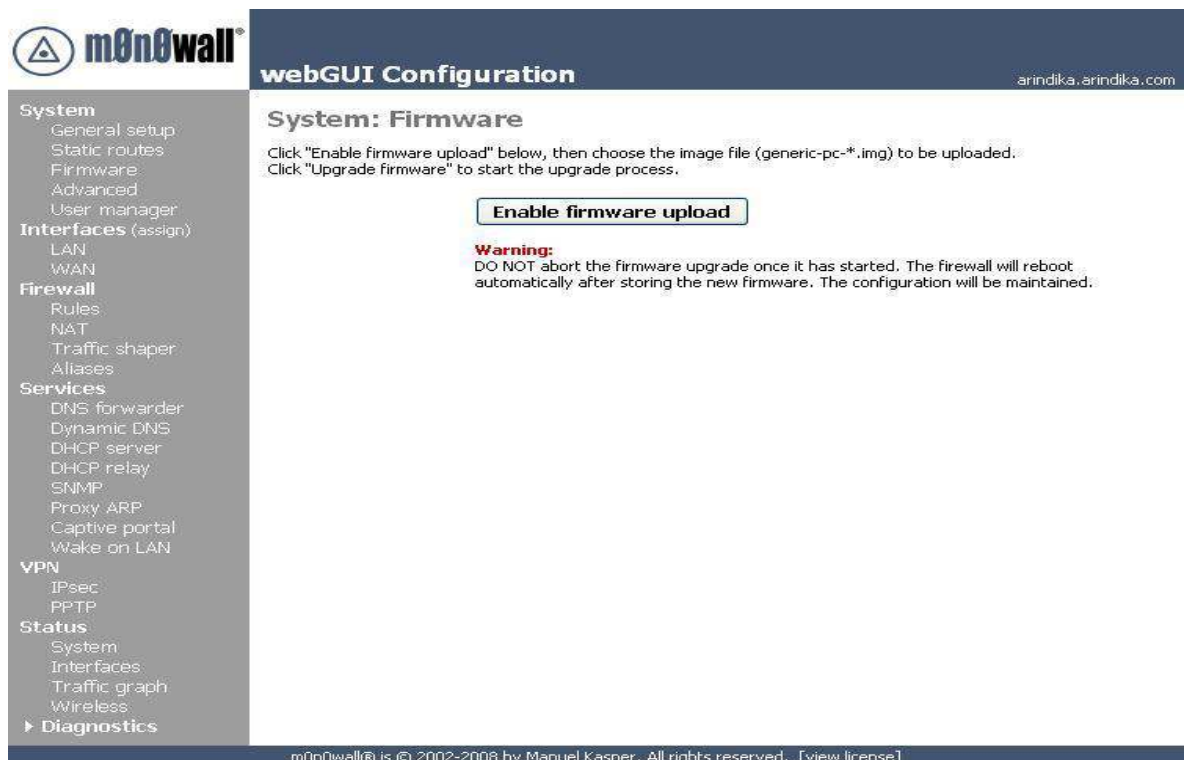
- System :
- General setup(sudah dibahas sebelumnya)
 - Static routes
 - Firmware
 - Advanced
 - User manager

Pengaturan static routes pada monowall



The screenshot shows the m0n0wall webGUI Configuration interface. The left sidebar contains a navigation menu with categories: System, Interfaces (assign), Firewall, Services, and VPN. The main content area is titled "System: Static routes" and features a table with columns: Interface, Network, Gateway, and Description. A plus sign icon is visible in the top right corner of the table area. The footer of the page reads: "m0n0wall® is © 2002-2009 by Manuel Kasper. All rights reserved. [view license]"

Pengaturan firmware pada monowall yang bertujuan untuk memperbaharui image binary terbaru



The screenshot shows the m0n0wall webGUI Configuration interface for the Firmware section. The left sidebar is identical to the previous screenshot. The main content area is titled "System: Firmware" and contains the following text: "Click 'Enable firmware upload' below, then choose the image file (generic-pc-*.img) to be uploaded. Click 'Upgrade firmware' to start the upgrade process." Below this text is a button labeled "Enable firmware upload". A warning message follows: "Warning: DO NOT abort the firmware upgrade once it has started. The firewall will reboot automatically after storing the new firmware. The configuration will be maintained." The footer of the page reads: "m0n0wall® is © 2002-2008 by Manuel Kasper. All rights reserved. [view license]"

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

m0n0wall® webGUI Configuration m0n0wall.local

System: Advanced setup

Note: the options on this page are intended for use by advanced users only, and there's **NO** support for them.

IPv6 support

Enable IPv6 support
After enabling IPv6 support, configure IPv6 addresses on your LAN and WAN interfaces, then add IPv6 firewall rules.

Save

Filtering bridge

Enable filtering bridge
This will cause bridged packets to pass through the packet filter in the same way as routed packets do (by default bridged packets are always passed). If you enable this option, you'll have to add filter rules to selectively permit traffic from bridged interfaces.

Save

webGUI SSL certificate/key

Certificate

Key

Paste a signed certificate in X.509 PEM format here.

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..

m0n0wall® webGUI Configuration arindika.arindika.com

System: User manager

Users **Groups**

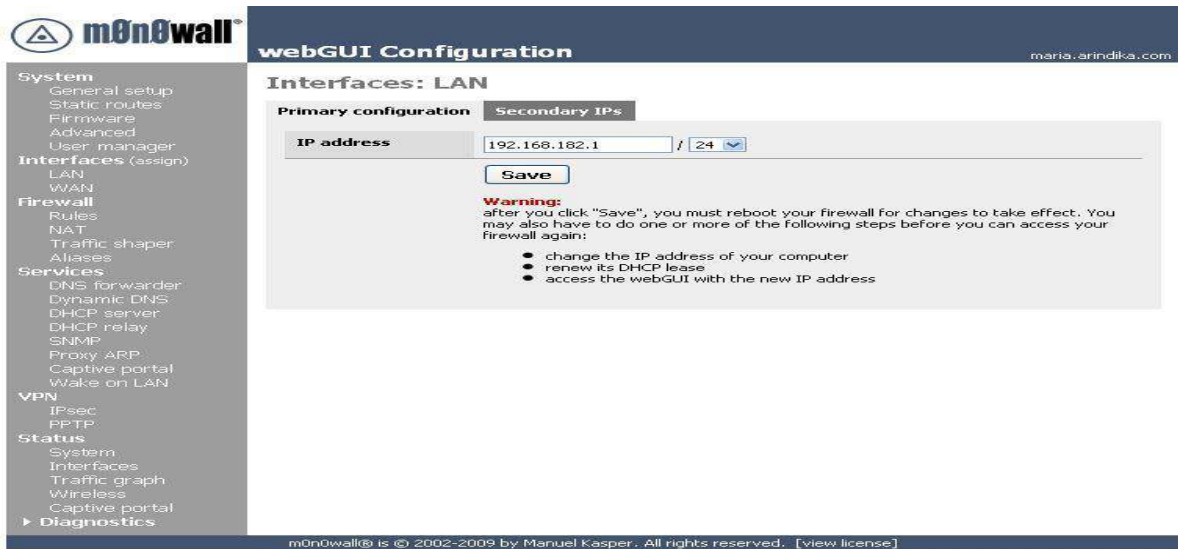
Username	Full name	Group
jessica	jessica patricia	cantique

Additional webGUI users can be added here. User permissions are determined by the admin group they are a member of.

m0n0wall® is © 2002-2008 by Manuel Kasper. All rights reserved. [view license]

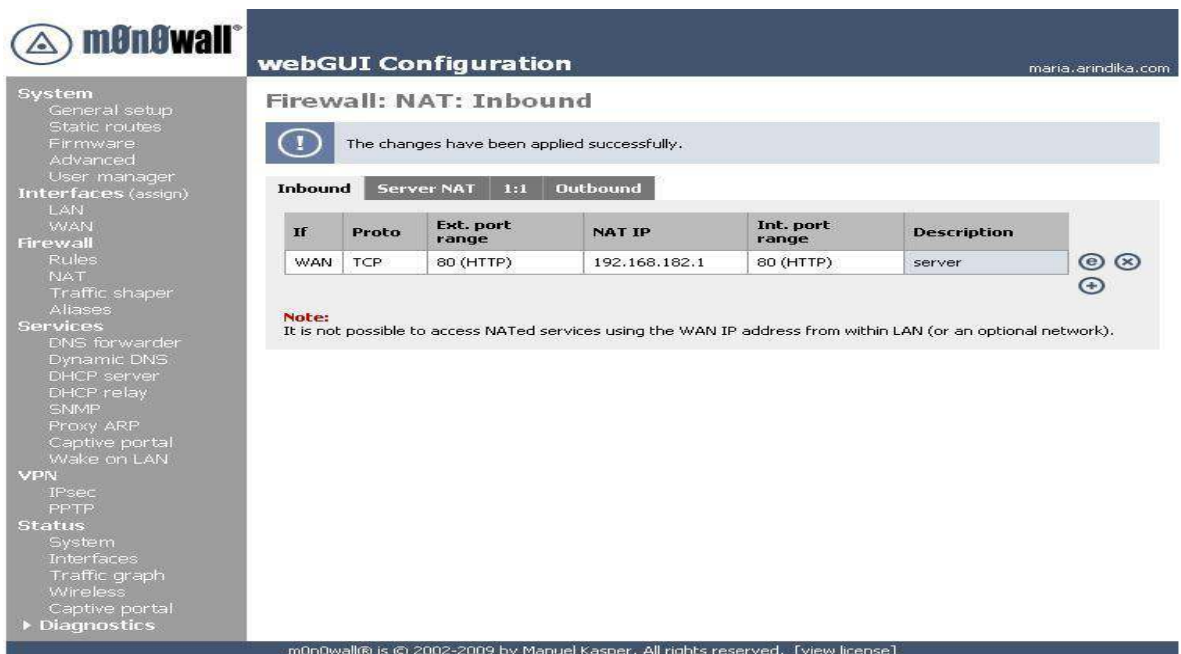
- Interfaces : • LAN
(assign)
- WAN(Pengaturan interface WAN telah dibahas sebelumnya)

Pengaturan interface LAN



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

Pengaturan NAT



Pengaturan traffic shaper

webGUI Configuration m0n0wall.local

Firewall: Traffic shaper: Rules

Rules Pipes Queues Magic shaper wizard

Enable traffic shaper

If	Proto	Source	Destination	Target	Description
WAN	TCP	*	*	m_High Priority #3 Upload	m_TCP ACK Upload
WAN	*	*	*	m_High Priority #1 Upload	m_Small Pkt Upload
WAN	UDP	*	* Port: 53 (DNS)	m_High Priority #1 Upload	m_Outbound DNS Query
WAN	AH	*	*	m_High Priority #1 Upload	m_AH Upload
WAN	ESP	*	*	m_High Priority #1 Upload	m_ESP Upload
WAN	GRE	*	*	m_High Priority #1 Upload	m_GRE Upload
WAN	ICMP	*	*	m_High Priority #2 Upload	m_ICMP Upload
WAN	*	*	*	m_Bulk Upload	m_Catch-All Upload

Pengaturan aliases

webGUI Configuration maria.arindika.com

Firewall: Aliases

The changes have been applied successfully.

Name	Address	Description
jasakom	119.2.43.84	situs jasakom

Note:
Aliases act as placeholders for real IP addresses and can be used to minimize the number of changes that have to be made if a host or network address changes. You can enter the name of an alias instead of an IP address in all address fields that have a blue background. The alias will be resolved to its current address according to the list below. If an alias cannot be resolved (e.g. because you deleted it), the corresponding element (e.g. filter/NAT/shaper rule) will be considered invalid and skipped.

m0n0wall® is © 2002-2009 by Manuel Kasper. All rights reserved. [view license]

- Services :
- DNS Forwarder
 - Dynamic DNS

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

Pengaturan DNS Forwarder

The screenshot shows the m0n0wall webGUI Configuration page for "Services: DNS forwarder". The left sidebar contains a navigation menu with categories like System, Interfaces, Firewall, Services, VPN, and Status. The main content area is titled "Services: DNS forwarder" and includes the following options:

- Enable DNS forwarder**
- Enable All Servers**
By default, when more than one upstream server is available, it will send queries to just one server. Setting this flag forces all queries to all available servers. The reply from the server which answers first will be returned to the original requestor.
- Register DHCP leases in DNS forwarder**
If this option is set, then machines that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in System: General setup to the proper value.

Below these options is a "Save" button and a "Note" section. The note states: "If the DNS forwarder is enabled, the DHCP service (if enabled) will automatically serve the LAN IP address as a DNS server to DHCP clients so they will use the forwarder. The DNS forwarder will use the DNS servers entered in System: General setup or those obtained via DHCP or PPP on WAN if the 'Allow DNS server list to be overridden by DHCP/PPP on WAN' is checked. If you don't use that option (or if you use a static IP address on WAN), you must manually specify at least one DNS server on the System: General setup page." Below the note, there is a table for overriding DNS forwarder results:

Host	Domain	IP	Description
Below you can override an entire domain by specifying an authoritative DNS server to be queried for that domain.			
Domain	IP	Description	

At the bottom of the page, it says "m0n0wall® is © 2002-2009 by Manuel Kasper. All rights reserved. [view license]"

Pengaturan Dynamic DNS

The screenshot shows the m0n0wall webGUI Configuration page for "Services: Dynamic DNS". The left sidebar is the same as in the previous screenshot. The main content area is titled "Services: Dynamic DNS" and includes the following options:

- Enable**
- Dynamic DNS client**
 - Service type:** DynDNS
 - Hostname:** [text input]
 - Server:** [text input] Special server to connect to. This can usually be left blank.
 - Port:** [text input] Special server port to connect to. This can usually be left blank.
 - MX:** [text input] Set this option only if you need a special MX record. Not all services support this.
 - Wildcards:** Enable Wildcard
 - Username:** [text input]
 - Password:** [text input]
- RFC 2136 Dynamic DNS updates**
 - Enable**
 - Hostname:** [text input]
 - TTL:** 60 seconds
 - Key name:** [text input] This must match the setting on the DNS server.
 - Key:** [text input] Paste an HMAC-MD5 key here.
 - Protocol:** Use TCP instead of UDP

Below these options is a "Save" button and a "Note" section. The note states: "You must configure a DNS server in System: General setup or allow the DNS server list to be overridden by DHCP/PPP on WAN for dynamic DNS updates to work."

Pengaturan DHCP server

m0n0wall webGUI Configuration maria.arindika.com

Services: DHCP server

LAN

Enable IPv4 DHCP server on LAN interface Enable

Deny unknown clients Only respond to reserved clients listed below.

Subnet 192.168.182.0

Subnet mask 255.255.255.0

Available range 192.168.182.1 - 192.168.182.254

Range to

WINS servers

Default lease time seconds
This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.

Maximum lease time seconds
This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.

Next server
Specify the server from which clients should load the boot file. This is usually only needed with PXE booting and some VoIP phones, and can usually be left empty.

Filename
Specify the name of the boot file on the server above. This is usually only needed with PXE booting and some VoIP phones, and can usually be left empty.

Note:
The DNS servers entered in System: General setup (or the DNS forwarder, if enabled) will be assigned to clients by the DHCP server.

The DHCP lease table can be viewed on the Diagnostics: DHCP leases page.

Reservations

Pengaturan DHCP relay

m0n0wall webGUI Configuration m0n0wall.local

Services: DHCP relay

LAN

Enable DHCP relay on LAN interface

Append circuit ID and agent ID to requests
If this is checked, the DHCP relay will append the circuit ID (m0n0wall interface number) and the agent ID to the DHCP request.

Destination server Proxy requests to DHCP server on WAN subnet:

This is the IP address of the server to which the DHCP packet is relayed. Select "Proxy requests to DHCP server on WAN subnet" to relay DHCP packets to the server that was used on the WAN interface.

m0n0wall® is © 2002-2008 by Manuel Kasper. All rights reserved. [\[view license\]](#)

Pengaturan SNMP

The screenshot shows the m0n0wall webGUI Configuration page for the 'Services: SNMP' section. The left sidebar contains a navigation menu with categories: System, Interfaces (assign), Firewall, Services, VPN, and Status. The main content area is titled 'Services: SNMP' and includes a checkbox for 'Enable SNMP agent'. Below this are three input fields: 'System location', 'System contact', and 'Community' (with the value 'public' and a note: 'In most cases, "public" is used here'). There is also a checkbox for 'Bind to LAN interface only' with a descriptive note. A 'Save' button is located at the bottom of the configuration area. The footer of the page reads: 'm0n0wall® is © 2002-2008 by Manuel Kasper. All rights reserved. [view license]'.

Pengaturan proxy ARP

The screenshot shows the m0n0wall webGUI Configuration page for the 'Services: Proxy ARP: Edit' section. The left sidebar contains a navigation menu with categories: System, Interfaces (assign), Firewall, Services, VPN, and Status. The main content area is titled 'Services: Proxy ARP: Edit' and includes a dropdown menu for 'Interface' (set to 'WAN'). Below this are three input fields: 'Network' (with a 'Type' dropdown set to 'Single address', an 'Address' field, and a 'Range' field with a '31' dropdown), and 'Description' (with a note: 'You may enter a description here for your reference (not parsed)'). A 'Save' button is located at the bottom of the configuration area. The footer of the page reads: 'm0n0wall® is © 2002-2008 by Manuel Kasper. All rights reserved. [view license]'.

Pengaturan Wake on LAN

The screenshot shows the m0n0wall webGUI Configuration page for "Services: Wake on LAN". The left sidebar contains a navigation menu with categories: System, Interfaces (assign), Firewall, Services, VPN, Status, and Diagnostics. The main content area has a title "Services: Wake on LAN" and a sub-section for configuring the service. It includes a dropdown menu for "Interface" (set to LAN) and a text input for "MAC address". A "Send" button is located below the input. A note explains that this service sends "Magic Packets" to wake up computers. Below the note is a table of MAC addresses for convenience.

Interface Choose which interface the host to be woken up is connected to.

MAC address Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx

Note:
This service can be used to wake up (power on) computers by sending special "Magic Packets". The NIC in the computer that is to be woken up must support Wake on LAN and has to be configured properly (WOL cable, BIOS settings).

You may store MAC addresses below for your convenience. Click the MAC address to wake up a computer.

Interface	MAC address	Description
LAN	00:21:00:5c:77:0f	mac address

m0n0wall@ is © 2002-2008 by Manuel Kasper. All rights reserved. [view license]

- VPN :
- IPsec
 - PPTP

Pengaturan IPsec

The screenshot shows the m0n0wall webGUI Configuration page for "VPN: IPsec: Tunnels". The left sidebar is the same as in the previous screenshot. The main content area has a title "VPN: IPsec: Tunnels" and a sub-section for configuring IPsec tunnels. It includes a checkbox for "Enable IPsec" and a "Save" button. Below this is a table for configuring tunnels.

Tunnels **Mobile clients** **Pre-shared keys** **CAs**

Enable IPsec

Local net	Remote net	Interface	Remote gw	P1 mode	P1 Enc. Algo	P1 Hash Algo	Description

m0n0wall@ is © 2002-2008 by Manuel Kasper. All rights reserved. [view license]

Pengaturan PPTP

System

- General setup
- Static routes
- Firmware
- Advanced
- User manager

Interfaces (assign)

- LAN
- WAN

Firewall

- Rules
- NAT
- Traffic shaper
- Aliases

Services

- DNS forwarder
- Dynamic DNS
- DHCP server
- DHCP relay
- SNMP
- Proxy ARP
- Captive portal
- Wake on LAN

VPN

- IPsec
- PPTP

Status

- System
- Interfaces
- Traffic graph
- Wireless

► **Diagnostics**

VPN: PPTP: Configuration

Configuration
Users

Off

Redirect incoming PPTP connections to:

PPTP redirection

Enter the IP address of a host which will accept incoming PPTP connections.

Enable PPTP server

Server address

Enter the IP address the PPTP server should use on its side for all clients.

Remote address range

Specify the start address and size for the client IP address subnet. The PPTP server will assign client addresses from the subnet given above to clients. The size of the subnet determines the maximum number of concurrent connections that the PPTP server can handle.

RADIUS

Use a RADIUS server for authentication
When set, all users will be authenticated using the RADIUS server specified below. The local user database will not be used.

Enable RADIUS accounting
Sends accounting packets to the RADIUS server.

RADIUS server

Enter the IP address of the RADIUS server.

RADIUS shared secret

Enter the shared secret that will be used to authenticate to the RADIUS server.

Require 128-bit encryption
When set, 128-bit encryption will be accepted. Otherwise, 40-bit and 56-bit encryption will be accepted, too. Note that encryption will always be forced on PPTP connections (i.e. unencrypted connections will not be accepted).

Note:
don't forget to add a firewall rule to permit traffic from PPTP clients!

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

Tampilan system

System

- General setup
- Static routes
- Firmware
- Advanced
- User manager

Interfaces (assign)

- LAN
- WAN

Firewall

- Rules
- NAT
- Traffic shaper
- Aliases

Services

- DNS forwarder
- Dynamic DNS
- DHCP server
- DHCP relay
- SNMP
- Proxy ARP
- Captive portal
- Wake on LAN

VPN

- IPsec
- PPTP

Status

- System
- Interfaces
- Traffic graph
- Wireless
- Captive portal

► **Diagnostics**

webGUI Configuration
arindika.arindika.com

System information

Name	arindika.arindika.com
Version	1.3b15 built on Sat Oct 11 18:48:10 CEST 2008
Platform	Generic PC
Uptime	00:32
Last config change	Mon Jan 17 14:45:23 WIT 2005
CPU usage	view graph
Memory usage	<div style="width: 80px; height: 10px; background: linear-gradient(to right, #444, #ccc);"></div> 8%
Notes	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div>

m0n0wall© is © 2002-2008 by Manuel Kasper. All rights reserved. [view license]

Mengetahui status interfaces

m0n0wall webGUI Configuration maria.arindika.com

System
 General setup
 Static routes
 Firmware
 Advanced
 User manager

Interfaces (assign)
 LAN
 WAN

Firewall
 Rules
 NAT
 Traffic shaper
 Aliases

Services
 DNS forwarder
 Dynamic DNS
 DHCP server
 DHCP relay
 SNMP
 Proxy ARP
 Captive portal
 Wake on LAN

VPN
 IPsec
 PPTP

Status
 System
 Interfaces
 Traffic graph
 Wireless
 Captive portal
 ▶ Diagnostics

Status: Interfaces

WAN interface	
Status	up
MAC address	00:10:b5:7b:2e:01
IPv4 address	10.252.108.6/255.255.255.240
IPv4 gateway	10.252.108.1
IPv6 address	fe80::210:b5ff:fe7b:2e01%r1/64
ISP DNS servers	192.168.2.1
Media	100baseTX <full-duplex>
In/out packets	807/534 (736 KB/59 KB)
In/out errors	0/0
Collisions	0

LAN interface	
Status	up
MAC address	00:21:91:17:8f:72
IPv4 address	192.168.182.1/255.255.255.0
IPv6 address	fe80::221:91ff:fe17:8f72%r0/64
Media	100baseTX <full-duplex>
In/out packets	1448/2136 (171 KB/1.70 MB)
In/out errors	0/0
Collisions	0

m0n0wall® is © 2002-2009 by Manuel Kasper. All rights reserved. [\[view license\]](#)

Mengetahui aktifitas download

m0n0wall webGUI Configuration m0n0wall.local

System
 General setup
 Static routes
 Firmware
 Advanced
 User manager

Interfaces (assign)
 LAN
 WAN

Firewall
 Rules
 NAT
 Traffic shaper
 Aliases

Services
 DNS forwarder
 Dynamic DNS
 DHCP server
 DHCP relay
 SNMP
 Proxy ARP
 Captive portal
 Wake on LAN

VPN
 IPsec
 PPTP

Status
 System
 Interfaces
 Traffic graph
 Wireless
 ▶ Diagnostics

Status: Traffic graph

Interface:

In 0 Kbps 12/9/2009 17:47:25 Switch to bytes/s
 Out 0 Kbps AutoScale (up)
 Graph shows last 120 seconds

75 Kbps
 50 Kbps
 25 Kbps

Note: if you can't see the graph, you may need to download the most recent version of the Firefox browser or install the Adobe SVG viewer.

m0n0wall® is © 2002-2008 by Manuel Kasper. All rights reserved. [\[view license\]](#)

Status wireless

The screenshot shows the m0n0wall webGUI Configuration interface. The top navigation bar includes the m0n0wall logo, the text "webGUI Configuration", and the IP address "m0n0wall.local". A left sidebar menu lists various configuration categories: System, Interfaces (assign), Firewall, Services, VPN, Status, and Diagnostics. The "Status" category is expanded, showing sub-items: System, Interfaces, Traffic graph, and Wireless. The "Wireless" sub-item is selected, displaying the "Status: Wireless" section. The main content area shows the text "Status: Wireless" followed by the message "No supported wireless interfaces were found for status display." At the bottom of the page, a footer contains the copyright information: "m0n0wall® is © 2002-2008 by Manuel Kasper. All rights reserved. [view license]"

- 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)

System

- General setup
- Static routes
- Firmware
- Advanced
- User manager

Interfaces (assign)

- LAN
- WAN

Firewall

- Rules
- NAT
- Traffic shaper
- Aliases

Services

- DNS forwarder
- Dynamic DNS
- DHCP server
- DHCP relay
- SNMP
- Proxy ARP
- Captive portal
- Wake on LAN

VPN

- IPsec
- PPTP

Status

- System
- Interfaces
- Traffic graph
- Wireless

▼ Diagnostics

- Logs
- DHCP Leases
- IPsec
- Ping/Traceroute
- ARP Table
- Firewall states
- Reset state

Diagnostics: Logs

System
Firewall
DHCP
Captive portal
PPTP VPN
Settings

Last 50 system log entries

Jan 16 01:16:21	kernel: kbd0 at atkbd0
Jan 16 01:16:21	kernel: atkbd0: [GIANT-LOCKED]
Jan 16 01:16:21	kernel: pmtimer0 on isa0
Jan 16 01:16:21	kernel: orm0: <ISA Option ROM> at iomem 0xcc000-0xd3fff on isa0
Jan 16 01:16:21	kernel: vga0: <Generic ISA VGA> at port 0x3c0-0x3df iomem 0xa0000-0xbffff on isa0
Jan 16 01:16:21	kernel: sc0: <System console> at flags 0x100 on isa0
Jan 16 01:16:21	kernel: sc0: VGA <16 virtual consoles, flags=0x300>
Jan 16 01:16:21	kernel: uhid0: vendor 0x15d9 USB Mouse, rev 1.10/1.00, addr 2, iclass 3/1
Jan 16 01:16:21	kernel: Timecounter "TSC" frequency 2412079587 Hz quality 800
Jan 16 01:16:21	kernel: Timecounters tick every 1.000 msec
Jan 16 01:16:21	kernel: Fast IPsec: Initialized Security Association Processing.
Jan 16 01:16:21	kernel: IP Filter: v4.1.28 initialized. Default = block all, Logging = enabled
Jan 16 01:16:21	kernel: md0: Preloaded image </mfsroot> 15728640 bytes at 0xc0a9c360
Jan 16 01:16:21	kernel: ad0: 39205MB <Maxtor 6E040L0 NAR61HA0> at ata0-master PIO4
Jan 16 01:16:21	kernel: acd0: CDROM <GIGABYTE GO-C5200C/7851> at ata1-slave PIO4
Jan 16 01:16:21	kernel: da0 at umass-sim0 bus 0 target 0 lun 0
Jan 16 01:16:21	kernel: da0: <Kingston DataTraveler 2.0 PMAP> Removable Direct Access SCSI-0 device
Jan 16 01:16:21	kernel: da0: 40.000MB/s transfers
Jan 16 01:16:21	kernel: da0: 1960MB (4014080 512 byte sectors: 255H 63S/T 249C)
Jan 16 01:16:21	kernel: Trying to mount root from ufs:/dev/md0
Jan 16 01:16:21	dnsmasq[133]: started, version 2.45 cachesize 150
Jan 16 01:16:21	dnsmasq[133]: compile time options: IPv6 GNU-getopt BSD-bridge ISC-leasefile no-DBus no-I18N TFTP
Jan 16 01:16:21	dnsmasq[133]: no servers found in /etc/resolv.conf, will retry
Jan 16 01:16:21	dnsmasq[133]: no servers found in /etc/resolv.conf, will retry

Penyewaan alamat IP

System

- General setup
- Static routes
- Firmware
- Advanced
- User manager

Interfaces (assign)

- LAN
- WAN

Firewall

- Rules
- NAT
- Traffic shaper
- Aliases

Services

- DNS forwarder
- Dynamic DNS
- DHCP server
- DHCP relay
- SNMP
- Proxy ARP
- Captive portal
- Wake on LAN

VPN

- IPsec
- PPTP

Status

- System
- Interfaces
- Traffic graph
- Wireless
- Captive portal

▼ Diagnostics

- Logs
- DHCP Leases
- IPsec
- Ping/Traceroute
- ARP Table
- Firewall states
- Reset state
- Backup/Restore

webGUI Configuration
maria.arindika.com

Diagnostics: DHCP leases

IP address	MAC address	Hostname	Start	End
192.168.182.10	00:22:64:4a:10:18	user-cbc66a5e63	2010/01/15 03:00:40	2010/01/15 05:00:40

Show active and expired leases

IPsec

The screenshot shows the m0n0wall webGUI Configuration interface. The top navigation bar includes the m0n0wall logo, the text "webGUI Configuration", and the URL "m0n0wall.local". A left sidebar menu lists various system settings such as System, Interfaces, Firewall, Services, and VPN. The main content area is titled "Diagnostics: IPsec" and features two tabs: "SAD" (selected) and "SPD". Below the tabs, a message states "No IPsec security associations."

Ping IP address

The screenshot shows the m0n0wall webGUI Configuration interface. The top navigation bar includes the m0n0wall logo, the text "webGUI Configuration", and the URL "maria.arindika.com". A left sidebar menu lists various system settings. The main content area is titled "Diagnostics: Ping" and features two tabs: "Ping" (selected) and "Traceroute". Below the tabs, there are input fields for "Host" (192.168.182.1), "Interface" (LAN), and "Count" (3). A "Ping" button is located below these fields. The "Ping output:" section displays the following text:

```
PING 192.168.182.1 (192.168.182.1) from 192.168.182.1: 56 data bytes
64 bytes from 192.168.182.1: icmp_seq=0 ttl=64 time=0.187 ms
64 bytes from 192.168.182.1: icmp_seq=1 ttl=64 time=0.099 ms
64 bytes from 192.168.182.1: icmp_seq=2 ttl=64 time=0.085 ms

--- 192.168.182.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.085/0.124/0.187/0.045 ms
```

ARP Table

The screenshot shows the m0n0wall webGUI Configuration interface. The left sidebar contains a navigation menu with categories: System, Interfaces (assign), Firewall, Services, VPN, and Status. The main content area is titled "Diagnostics: ARP table" and displays a table with the following data:

IP address	MAC address	Hostname	Interface
10.252.108.1	00:90:08:a3:6d:c5		WAN
192.168.182.10	00:22:64:4a:10:18	user-cbc66a5e63	LAN

Below the table, there is a "Hint" section: "IP addresses are resolved to hostnames if 'Resolve IP addresses to hostnames' is checked on the Diagnostics: Logs page."

Firewall states

The screenshot shows the m0n0wall webGUI Configuration interface. The left sidebar contains a navigation menu with categories: System, Interfaces (assign), Firewall, Services, VPN, and Status. The main content area is titled "Diagnostics: Firewall states" and displays a "Statistics snapshot control" section with a "Start new" button and "Last statistics snapshot: Never". Below this is a table showing firewall connection states:

Source	Port	Destination	Port	Protocol	Packets	Bytes	TTL
192.168.182.10	3328	192.168.182.1	80	tcp	3	624	2:30:00

Below the table, it states "Firewall connection states displayed: 1".

Reset states

The screenshot shows the m0n0wall webGUI Configuration interface. The left sidebar contains a navigation menu with categories: System, Interfaces (assign), Firewall, Services, VPN, and Status. The main content area is titled "Diagnostics: Reset state" and displays two checked options: "NAT table" and "Firewall state table". Below these options, there is a text block explaining the reset process:

Resetting the state tables will remove all entries from the corresponding tables. This means that all open connections will be broken and will have to be re-established. This may be necessary after making substantial changes to the firewall and/or NAT rules, especially if there are IP protocol mappings (e.g. for PPTP or IPv6) with open connections.

The firewall will normally leave the state tables intact when changing rules.

NOTE: If you reset the firewall state table, the browser session may appear to be hung after clicking "Reset". Simply refresh the page to continue.

At the bottom of the page, there is a "Reset" button.

Backup and restore

The screenshot shows the m0n0wall webGUI Configuration interface. The left sidebar contains a navigation menu with categories: System, Interfaces (assign), Firewall, Services, VPN, Status, and Diagnostics. The main content area is titled "Diagnostics: Backup/restore". It is divided into two sections: "Backup configuration" and "Restore configuration".

Backup configuration: A button labeled "Download configuration" is present, with the instruction: "Click this button to download the system configuration in XML format."

Restore configuration: A "Browse..." button is used to select an XML file. Below it is a "Restore configuration" button. A note states: "Note: The firewall will reboot after restoring the configuration."

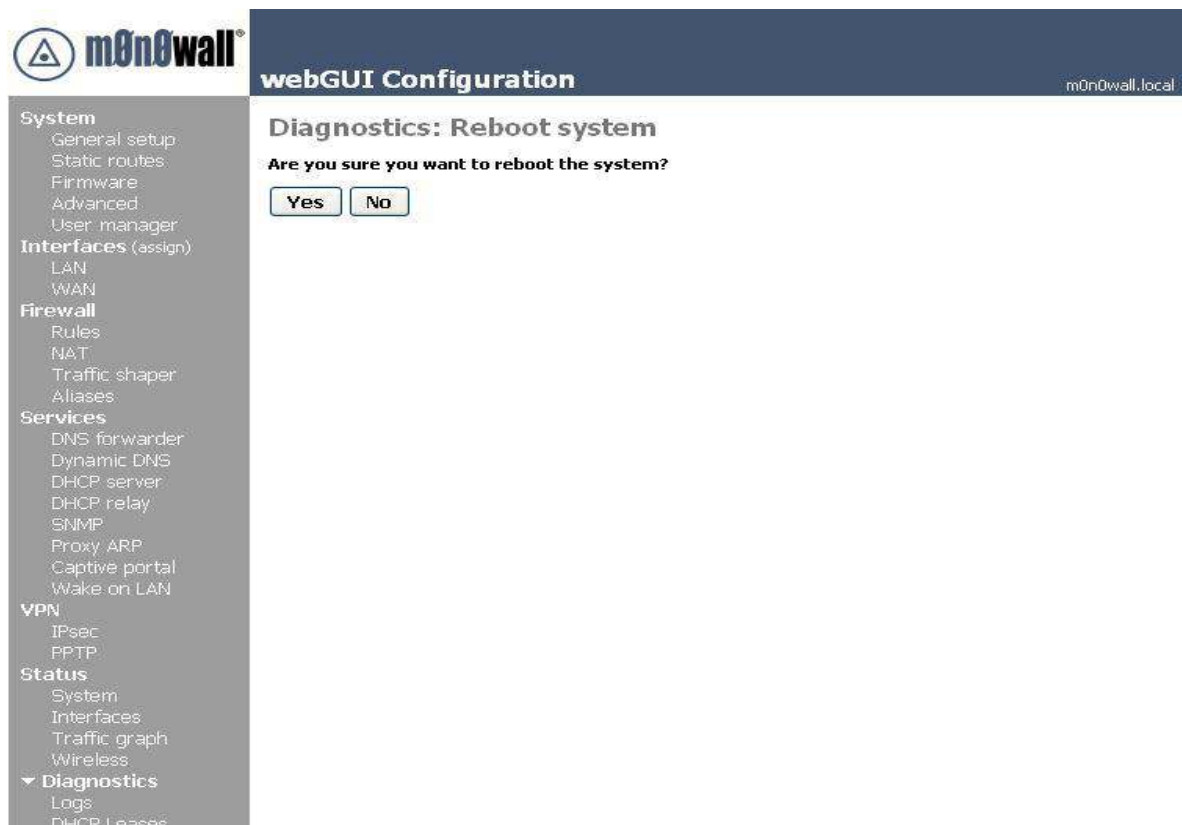
Factory defaults

The screenshot shows the m0n0wall webGUI Configuration interface. The left sidebar contains a navigation menu with categories: System, Interfaces (assign), Firewall, Services, VPN, Status, and Diagnostics. The main content area is titled "Diagnostics: Factory defaults".

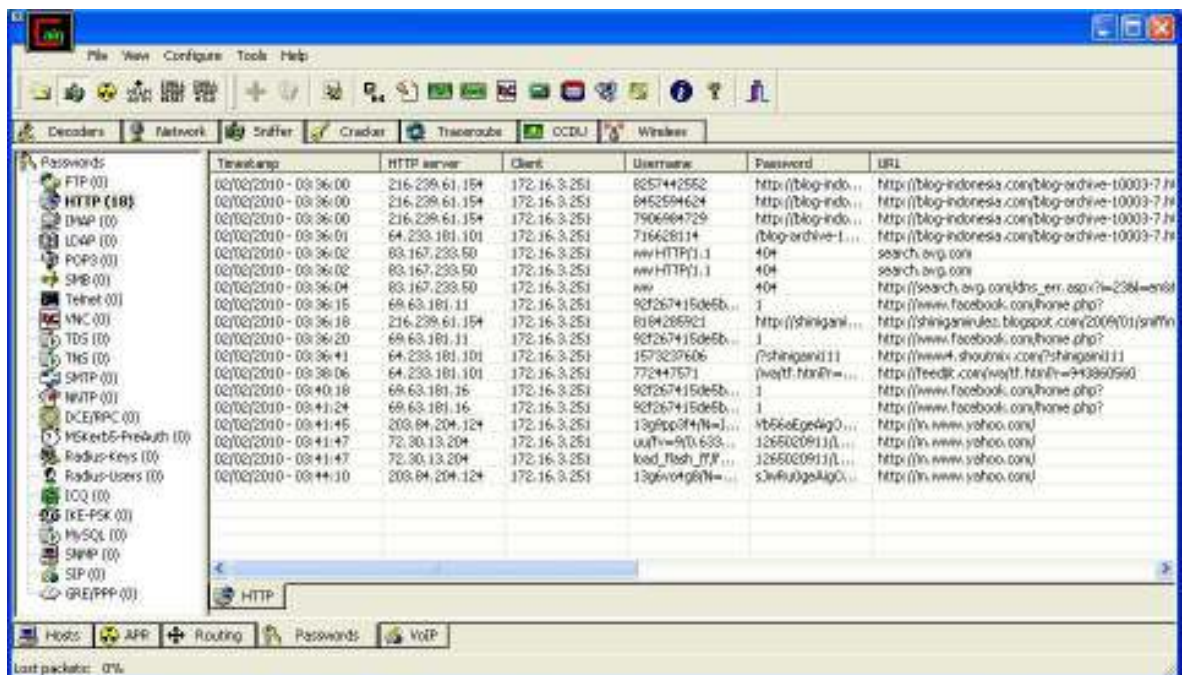
The main content area contains a warning: "If you click 'Yes', the firewall will be reset to factory defaults and will reboot immediately. The entire system configuration will be overwritten. The LAN IP address will be reset to 192.168.1.1, the system will be configured as a DHCP server, and the password will be set to 'mono'."

Below the warning is a confirmation question: "Are you sure you want to proceed?" with two buttons: "Yes" and "No".

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 memiliki 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.

```
*NOTE*  pfSense requires *AT LEAST* 2 assigned interfaces to function.
        If you do not have two interfaces you CANNOT continue.

        If you do not have at least two *REAL* network interface cards
        or one interface with multiple VLANs then pfSense *WILL NOT*
        function correctly.

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

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

Do you want to proceed [y|n]?y
```

```
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 [yin]? 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).

The screenshot shows the Sense webConfigurator interface. The top navigation bar includes the Sense logo, the text "webConfigurator", and a "Help" link. A sidebar on the left lists various configuration categories: System, Interfaces, Firewall, Services, and VPN. The main content area is titled "Interfaces: WAN" and is divided into several sections:

- General configuration:**
 - Type: Static (selected)
 - MAC address: [input field] Copy my MAC address. A note explains this field can be used to "spoof" the MAC address.
 - MTU: [input field]. A note explains that entering a value here affects MSS clamping for TCP connections.
- Static IP configuration:**
 - IP address: 10.252.108.7 / 24
 - Gateway: 10.252.108.1
- DHCP client configuration:**
 - Hostname: [input field]. A note explains this value is sent as the DHCP client identifier.
- PPPoE configuration:**
 - Username: [input field]
 - Password: [input field]
 - Service name: [input field]. A hint indicates this field can usually be left empty.
- WAN:**
 - Dial on demand: Enable Dial-on-Demand mode

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.

- 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
- siproxd
- Proxy server
- Antivirus
- VPN**
- IPsec
- OpenVPN
- PPTP
- L2TP
- Status

Services: Captive portal



The changes have been applied successfully. You can also [monitor](#) the filter reload progress.

Captive portal

Pass-through MAC

Allowed IP addresses

File Manager

Enable captive portal

Interface	<input type="text" value="WAN"/> <p>Choose which interface to run the captive portal on.</p>
Maximum concurrent connections	<input type="text"/> per client IP address (0 = no limit) <p>This setting limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many users can load the portal page or authenticate at the same time! Default is 4 connections per client IP address, with a total maximum of 16 connections.</p>
Idle timeout	<input type="text"/> minutes <p>Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.</p>
Hard timeout	<input type="text" value="60"/> minutes <p>Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).</p>
Logout popup window	<input type="checkbox"/> Enable logout popup window <p>If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.</p>
Redirection URL	<input type="text"/> <p>If you provide a URL here, clients will be redirected to that URL instead of the one they initially tried to access after they've authenticated.</p>
Concurrent user logins	<input type="checkbox"/> Disable concurrent logins <p>If this option is set, only the most recent login per username will be active. Subsequent logins will cause machines previously logged in with the same username to be disconnected.</p>
MAC filtering	<input checked="" type="checkbox"/> Disable MAC filtering <p>If this option is set, no attempts will be made to ensure that the MAC address of clients stays the same while they're logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pfSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used.</p>
Per-user bandwidth restriction	<input type="checkbox"/> Enable per-user bandwidth restriction

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

Advanced

The screenshot shows the pSense webConfigurator interface. The top navigation bar includes the pSense logo, the title "webConfigurator", and a "Subject Window" button. A left sidebar contains a menu with categories: System (Advanced, Firmware, General Setup, Packages, Setup Wizard, Static routes), Interfaces (assign), WAN, LAN, Firewall (Aliases, NAT, Rules, Schedules, Traffic Shaper, Virtual IPs), Services (Captive portal, DNS forwarder, DHCP relay, DHCP server, Dynamic DNS, Load Balancer, OLSR, PPPoE Server, RIP, SNMP, UPnP, OpenNTPD, Wake on LAN, speed, Antivirus, Speed, Proxy server, Proxy filter), and VPN (IPsec, OpenVPN). The main content area is titled "System: Advanced functions". A red notification banner at the top states: "The changes have been applied successfully. You can also [cancel](#) the filter reload progress." Below this, a note reads: "Notes: the options on this page are intended for use by advanced users only." The "Enable Serial Console" section has a checkbox for "This will enable the first serial port with 9600/8/N/1." and a note: "Note: This will disable the internal video card/keyboard." The "Secure Shell" section has a checked checkbox for "Enable Secure Shell" and an unchecked checkbox for "Disable Password login for Secure Shell (KEY only)". The "SSH port" field is empty, with a note: "Note: Leave this blank for the default of 22." The "Authorizedkeys" section has a large text area and a note: "Paste an authorized keys file here." Both sections have "Save" buttons.

Firmware

The screenshot shows the pSense webConfigurator interface for the "Diagnostics: Firmware" section. The top navigation bar includes the pSense logo, the title "webConfigurator", and the URL "maria.pfsense.com". The left sidebar menu is partially visible, showing "System" and "Firmware" options. The main content area is titled "Diagnostics: Firmware" and has three tabs: "Manual Update", "Auto Update", and "Update Settings". The "Manual Update" tab is active. A red banner at the top of the content area says "Invoke pSense Manual Upgrade". Below this, there is a checkbox labeled "Enable firmware upload" and a "Save" button. A note reads: "Click 'Enable firmware upload' below, then choose the image file (pSense-*.img) to be uploaded. Click 'Upgrade firmware' to start the upgrade process." A "Warning" section follows, stating: "DO NOT abort the firmware upgrade once it has started. The firewall will reboot automatically after storing the new firmware. The configuration will be maintained."

General setup

The screenshot shows the 'System: General Setup' page in the pfSense webConfigurator. The left sidebar contains a navigation menu with categories: System, Interfaces, Firewall, and Services. The main content area is a form with the following fields:

- Hostname:** Input field with 'maria'. Description: name of the firewall host, without domain part e.g. firewall
- Domain:** Input field with 'arindika.com'. Description: e.g. mycorp.com
- DNS servers:** Input field with '192.168.2.1'. Description: IP addresses; these are also used for the DHCP service, DNS forwarder and for PPPoE clients. A checkbox is checked: **Allow DNS server list to be overridden by DHCP/PPP on WAN**. Description: If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). They will not be assigned to DHCP and PPPoE WAN clients, though.
- Username:** Input field with 'admin'. Description: If you want to change the username for accessing the webGUI, enter it here.
- Password:** Two input fields for password and confirmation. Description: If you want to change the password for accessing the webGUI, enter it here twice.
- webGUI protocol:** Radio buttons for HTTP (selected) and HTTPS.
- webGUI port:** Input field. Description: Enter a custom port number for the webGUI above if you want to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.
- Time zone:** Dropdown menu with 'Asia/Jakarta' selected. Description: Select the location closest to you.
- NTP time server:** Input field with '0.pool.ntp.org'. Description: Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if you enter a host name here!

Packages

The screenshot shows the 'System: Package Manager' page in the pfSense webConfigurator. The left sidebar is the same as in the previous screenshot. The main content area shows a table of available packages:

Package Name	Category	Package Info	Package Version	Description
HAAP-antivirus	Network Management	No info, check the forum		Antivirus: HAAP (HTTP Antivirus Proxy) is a proxy with a ClamAV anti-virus scanner. The main aims are: continuous, non-blocking downloads and in-depth scanning of dynamic and password-protected HTTP traffic. Help antivirus proxy has a parent and transparent proxy mode. It can be used with squid or standalone. And File Scanner for local files.
sgroup	Services	No info, check the forum		Proxy for handling NAT of multiple ISP devices to a single public IP.
squid	Network	No info, check the forum		High performance web proxy cache.

At the top of the package list, there are tabs for 'Available 2.8-ALPHA-ALPHA packages', 'Packages for any platform', and 'Installed packages'. On the right side of the table, there are icons for each package, including a red 'X' icon for HAAP-antivirus.

Setup wizard



On this screen you will set the General pfSense parameters.

General Information	
Hostname:	<input type="text" value="maria"/> EXAMPLE: myserver
Domain:	<input type="text" value="arindika.com"/> EXAMPLE: mydomain.com
Primary DNS Server:	<input type="text" value="192.168.2.1"/>
Secondary DNS Server:	<input type="text"/>

Next

Static routes

The screenshot shows the pfSense webConfigurator interface. The top navigation bar includes the pfSense logo, the title "webConfigurator", and a status bar with the text "pfSense 2.3.4-RELEASE.1 [01-13-10 20:05:25 - 192.168.1.1]". A left sidebar menu lists various system settings, with "Static routes" selected. The main content area is titled "System: Static Routes" and features a table with columns for "Interface", "Network", "Gateway", and "Description". Below the table, a note states: "Note: Do not enter static routes for networks assigned on any interface of this firewall. Static routes are only used for networks reachable via a different router, and not reachable via your default gateway."

- Interfaces :
- WAN(interface WAN telah dibahas sebelumnya)
 - LAN

LAN

The screenshot shows the Sense webConfigurator interface for configuring the LAN interface. The left sidebar contains a navigation menu with categories: System, Interfaces, Firewall, and Services. The main content area is titled "Interfaces: LAN" and includes sections for "IP configuration" and "FTP Helper".

IP configuration

- Bridge with: none
- IP address: 102.168.1.5 / 24

FTP Helper

- Disable the userland FTP-Proxy application

Save

Warning: after you click "Save", you will need to do one or more of the following steps before you can access your firewall again:

- change the IP address of your computer
- renew its DHCP lease
- access the webGUI with the new IP address
- be sure to add **firewall** rules to permit traffic through the interface.
- We also need **firewall** rules for an interface in behind mode as the firewall acts as a filtering bridge.

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

Aliases

The screenshot shows the Sense webConfigurator interface for configuring Firewall Aliases. The left sidebar contains a navigation menu with categories: System, Interfaces, Firewall, and Services. The main content area is titled "Firewall: Aliases" and includes a success message and a table of aliases.

The changes have been applied successfully. You can also [refresh](#) the filter reload progress.

Name	Values	Description
isolated	119.2.43.84	stop hacker

Notes:
Aliases act as placeholders for real hosts, networks or ports. They can be used to minimize the number of changes that have to be made if a host, network or port changes. You can enter the name of an alias instead of the host, network or port in all fields that have a red background. The alias will be resolved according to the list above. If an alias cannot be resolved (e.g. because you deleted it), the corresponding element (e.g. filter(NAT/shaper rule) will be considered invalid and skipped.

NAT

The screenshot shows the 'Firewall: NAT: Port Forward' configuration page in the Sense webConfigurator. The interface includes a sidebar with navigation options like System, Interfaces, and Firewall. The main content area features a 'Port Forward' section with a table for configuring NAT rules. The table has columns for 'Proto', 'Ext. port range', 'NAT IP', 'Int. port range', and 'Description'. A 'Port Forward' button is visible above the table.

Rules

The screenshot displays the 'Firewall: Rules' configuration page. A red notification banner at the top states: 'The settings have been applied. The firewall rules are now reloading in the background. You can also monitor the reload progress.' Below this, there are tabs for 'LAN' and 'WAN'. A table lists firewall rules with columns for 'Proto', 'Source', 'Port', 'Destination', 'Port', 'Gateway', 'Schedule', and 'Description'. Two rules are visible: one for 'LAN net' and another for 'TOP'. A legend at the bottom explains the status of various actions: pass, pass (disabled), block, block (disabled), reject, reject (disabled), log, and log (disabled). A 'Hint' section notes that rules are evaluated on a first-match basis.

Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
*	LAN net	*	*	*	*		Default LAN -> any
TOP	*	*	119.2.43.84	*	*		Default LAN -> any

Schedules

The screenshot shows the 'Firewall: Schedules' configuration page. It features a table with columns for 'Name', 'Time Range(s)', and 'Description'. One schedule is listed: 'routerAnn' with a time range from 'December 3' to 'December 25' and a 'jen' user. A 'Note' at the bottom states: 'Schedules act as placeholders for time ranges to be used in Firewall Rules.'

Name	Time Range(s)	Description
routerAnn	December 3 December 25	jen router/adjval

Traffic shaper



Shaper configuration

pfSense Traffic Shaper Wizard

Setup network speeds

Inside:	<input type="text" value="LAN"/> This is usually the LAN interface Inside interface for shaping your download speeds
Download:	<input type="text" value="50"/> The download speed of your WAN link in Kbits/second. Note: PPPOE users should take into account PPPOE overhead and put a lower speed here.
Outside:	<input type="text" value="WAN"/> This is usually the WAN interface Outside interface for shaping your upload speeds
Upload:	<input type="text" value="60"/> The upload speed of your WAN link in Kbits/second. Note: PPPOE users should take into account PPPOE overhead and put a lower speed here.

Virtual IPs

The screenshot shows the pfSense webConfigurator interface. The top navigation bar includes the Sense logo and the text "webConfigurator". A sidebar on the left contains a menu with categories: System, Interfaces, Firewall, Services, and VPN. The main content area is titled "Firewall: Virtual IP Addresses" and has two tabs: "Virtual IPs" (selected) and "CARP Settings". Below the tabs is a table with columns "Virtual IP address", "Type", and "Description". A note below the table states: "Note: The virtual IP addresses defined on this page may be used in NAT mappings. You can check the status of your CARP Virtual IPs and interfaces here."

- 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

The screenshot shows the Mikrotik WinBox webConfigurator interface. The top navigation bar includes the Mikrotik logo, the text "Sense webConfigurator", and the URL "mikrotik.or.id/ka.com". A left-hand sidebar menu lists various system settings categories: System, Interfaces, Firewall, and Services. The "Services" category is expanded, showing options like Captive Portal, DNS Forwarder, DHCP Relay, etc. The main content area is titled "Services: DNS forwarder" and contains the following configuration options:

- Enable DNS forwarder
- Register DHCP leases in DNS forwarder
If this option is set, then machines that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in System: General setup to the proper value.
- Register DHCP static mappings in DNS forwarder
If this option is set, then DHCP static mappings will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in System: General setup to the proper value.

Below these options is a "Save" button. A "Note:" section follows, stating: "If the DNS forwarder is enabled, the DHCP service (if enabled) will automatically serve the LAN IP address as a DNS server to DHCP clients so they will use the forwarder. The DNS forwarder will use the DNS servers entered in System: General setup or those obtained via DHCP or PPP on WAN if the 'allow DNS server list to be overridden by DHCP/PPP on WAN' is checked. If you don't use that option (or if you use a static IP address on WAN), you must manually specify at least one DNS server on the System: General setup page." Below the note, it says "You may enter records that override the results from the forwarders below." At the bottom, there is a table header with columns: Host, Domain, IP, and Description.

DHCP relay

Sense webConfigurator mantis.mikrotik.com

Services: DHCP Relay

DHCP Server is currently enabled. Cannot enable the DHCP Relay service while the DHCP Server is enabled on any interface.

DHCP Server

Services: DHCP server

! The DHCP Server can only be enabled on interfaces configured with static IP addresses.
The interfaces not configured with static ip will not be shown.

LAN

Enable DHCP server on LAN interface

Deny unknown clients
If this is checked, only the clients defined below will get DHCP leases from this server.

Subnet	192.168.182.0
Subnet mask	255.255.255.0
Available range	192.168.182.0 - 192.168.182.255
Range	192.168.182.10 to 192.168.182.245
WINS servers	<input type="text"/>
DNS servers	<input type="text"/> <small>NOTE: leave blank to use the system default DNS servers - this interface's IP if DNS forwarder is enabled, otherwise the servers configured on the General page.</small>
Gateway	<input type="text"/> <small>The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for your network.</small>
Domain-Name	<input type="text"/> <small>The default is to use the domainname of the router as DNS-Search string that is served via DHCP. Specify an alternate DNS-Search string here.</small>
Domain-Searchlist	<input type="text"/> <small>DNS-Searchlist: the DHCP server can serve a list of domains to be searched.</small>
Default lease time	<input type="text"/> seconds <small>This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.</small>
Maximum lease time	<input type="text"/> seconds <small>This is the maximum lease time for clients that ask for a specific expiration time.</small>

Dynamic DNS

The screenshot shows the MikroTik WinBox webConfigurator interface. The top navigation bar includes the Sense logo, 'webConfigurator', and the URL 'mario.arkindia.com'. A left sidebar contains a menu with categories: System, Packages, Interfaces, Firewall, and VPN. The main content area is titled 'Services: Dynamic DNS clients'. Under the 'DynDNS' tab, there is a table with the following data:

Service	Hostname	Cached IP	Description
WAN	DNS-O-Matic	mario.arkindia.com	MyHome

Below the table, a note states: 'Notes: IP addresses appearing in green are up to date with Dynamic DNS provider.'

Load balancer

The screenshot shows the MikroTik WinBox webConfigurator interface. The top navigation bar includes the Sense logo, 'webConfigurator', and the URL 'mario.arkindia.com'. A left sidebar contains a menu with categories: System, Packages, Interfaces, Firewall, and VPN. The main content area is titled 'Services: Load Balancer: Pool'. Under the 'Pool' tab, there is a table with the following data:

Name	Servers	Port	Monitor	Description

OLSR

The screenshot shows the MikroTik WinBox webConfigurator interface. The top navigation bar includes the Sense logo, 'webConfigurator', and the URL 'mario.arkindia.com'. A left sidebar contains a menu with categories: Packages, Interfaces, Firewall, and VPN. The main content area is titled 'OLSRD Settings'. The configuration options are as follows:

- Enable OLSR:** Enables the dynamic mesh linking daemon.
- Link Quality Level:**
- Interfaces:** Select the interfaces that OLSR will bind to. You can use the CTRL or COMMAND key to select multiple interfaces.
- Enable HTTPInfo Plugin:** Enables the OLSR stats web server.
- HTTPInfo Port:** Port that HTTPInfo will listen on.
- Allowed host(s):** Hosts that are allowed to access the HTTPInfo web service.
- Allowed host(s) subnet:** Enter the subnet mask in form 255.255.255.0
- Enable Dynamic Gateway:** Enables the OLSR Dynamic Gateways feature.
- Announce self as Dynamic Gateway:** Enables the OLSR Dynamic Gateways Announcing feature.
- Announce Dynamic local route:** Enter the IPNetwork.
- Ping:** Ping the host to ensure connectivity.
- poll:** How often to look for a neighbor, in seconds.
- Enable Secure Mode:** Enables the secure mode.
- Key:**

PPPoE server

- 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
- siproxd
- Proxy server
- Antivirus
- VPN**
- IPsec
- OpenVPN
- PPTP
- L2TP
- Status**
- Captive Portal

Services: PPPoE Server

Configuration
Users

Off

 Enable PPPoE server

Interface	WAN
Subnet netmask	0.0.0.0 <small>Hint: 24 is 255.255.255.0</small>
No. PPPoE users	0 <small>Hint: 10 is TEN pppoe clients</small>
Server address	<input type="text"/> <small>Enter the IP address the PPPoE server should use on its side for all clients.</small>
Remote address range	<input type="text"/> <small>Specify the starting address for the client IP address subnet.</small>
DNS servers	<input type="text"/> <small>If entered they will be given to all pppoe clients else lan dns and one wan dns will go to all clients</small>
RADIUS	<input type="checkbox"/> Use a RADIUS server for authentication <small>When set, all users will be authenticated using the RADIUS server specified below. The local user database will not be used.</small> <input type="checkbox"/> Enable RADIUS accounting <small>Sends accounting packets to the RADIUS server.</small> <input type="checkbox"/> Use Backup Radius Server <small>When set, if primary server fails all requests will be sent via backup server</small>
NAS IP ADDRESS	<input type="text"/> <small>radius server NAS ip Address</small>
Radius Accounting Update	<input type="text"/> <small>Radius accounting update period in seconds</small>
RADIUS issued IP's	<input type="checkbox"/> <small>Issue IP Addresses via RADIUS server.</small>
RADIUS server Primary	<input type="text"/> <input type="text"/> <input type="text"/> <small>Enter the IP address and portof the RADIUS server. Format ip auth_port acct_port</small>

RIP

Sense

webConfigurator

maria.or.india.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

Services: RIP

ROUTED Settings

Enable RIP	<input checked="" type="checkbox"/> <small>Enables the Routing Information Protocol daemon</small>
Interfaces	WAN LAN <small>Select the interfaces that RIP will bind to. You can use the CTRL or COMMAND key to select multiple interfaces.</small>
RIP Version	RIP Version 2 <small>Select which RIP version the daemon will listen/advertise using.</small>
RIPv2 password	pfSense <small>Specify a RIPv2 password. This password will be sent in the clear on all RIPv2 responses received and sent.</small>

SNMP

Sense webConfigurator maria@indika.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
 speed

Services: SNMP Enable

SNMP Daemon

Polling Port:
Enter the port to accept polling events on (default 161)

System location:

System contact:

Read Community String:
In most cases, "public" is used here.

SNMP Traps Enable

Trap server:
Enter trap server name

Trap server port:
Enter the port to send the traps to (default 162)

Enter the SNMP trap string:
Trap string

Modules

SNMP Modules

MibII
 Netgraph
 RFP
 Host Resources

UPnP

Sense webConfigurator maria@indika.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
 speed
 Proxy server
 Antivirus

VPN
 IPsec
 OpenVPN

Services: UPnP

UPnP Settings

Enable UPnP:

Interfaces (generally LAN):
You can use the CTRL or COMMAND key to select multiple interfaces.

Maximum Download Speed (bits/second):

Maximum Upload Speed (Kbits/second):

Override WAN address:

Log packets handled by UPnP rules?:

Use system updates instead of UPnP service updates?:

By default deny access to UPnP?:

User specified permissions 1:
Format: [allow or deny][ext port or range][int ipaddr or ipaddr/cidr] [int port or range]
 Example: allow 1024-65535 192.168.0.0/24 1024-65535

User specified permissions 2:
Format: [allow or deny][ext port or range][int ipaddr or ipaddr/cidr] [int port or range]

User specified permissions 3:
Format: [allow or deny][ext port or range][int ipaddr or ipaddr/cidr] [int port or range]

User specified permissions 4:
Format: [allow or deny][ext port or range][int ipaddr or ipaddr/cidr] [int port or range]

OpenNTPD

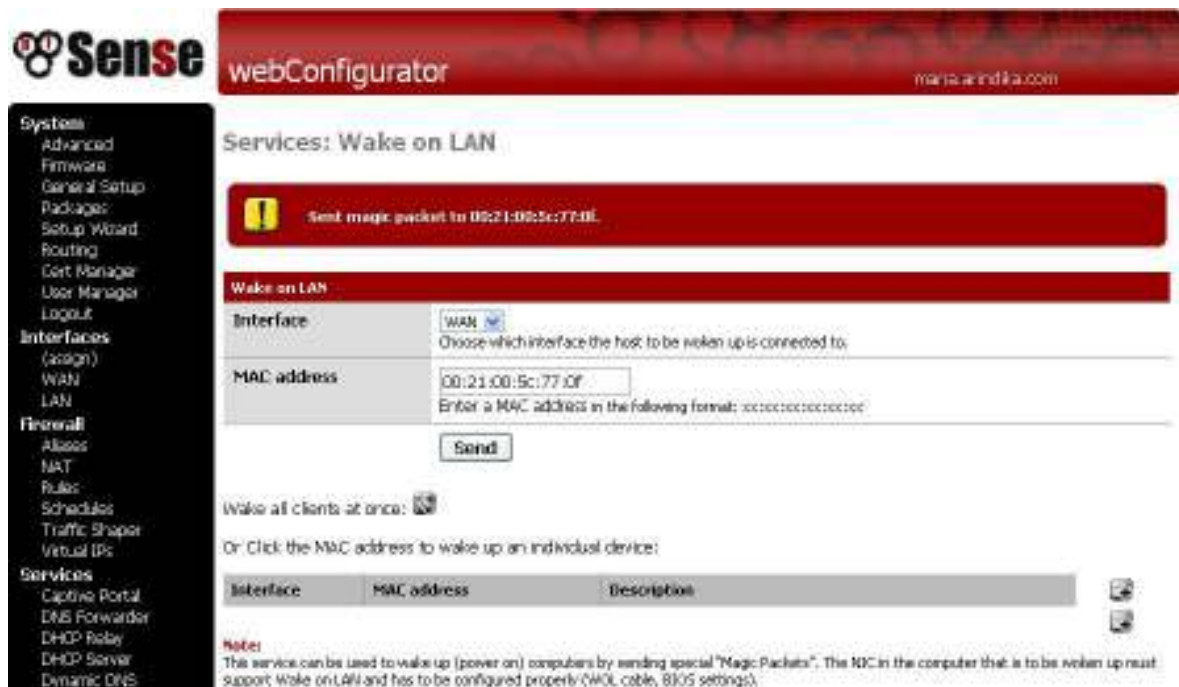


The screenshot shows the Senseware webConfigurator interface. The top header is red with the Senseware logo and "webConfigurator" text. A sidebar on the left lists navigation options under "System" and "Interfaces". The main content area is titled "NTP server" and contains a form with the following fields:

- Enable:** A checkbox that is checked, with the text "Check this to enable the NTP server."
- Interface:** A dropdown menu with "WAN" selected. Below it is the text "Select the interface(s) the NTP server will listen on."

A "Save" button is located at the bottom of the form.

Wake on LAN



The screenshot shows the Senseware webConfigurator interface for "Services: Wake on LAN". The top header is red with the Senseware logo and "webConfigurator" text. A sidebar on the left lists navigation options under "System", "Interfaces", "Firewall", and "Services". The main content area is titled "Services: Wake on LAN" and contains the following elements:

- A red banner with a yellow warning icon and the text "Send magic packet to 08:01:00:5c:77:0f".
- A section titled "Wake on LAN" with a sub-section "Wake on LAN" containing a form with the following fields:
 - Interface:** A dropdown menu with "WAN" selected. Below it is the text "Choose which interface the host to be woken up is connected to."
 - MAC address:** A text input field containing "00:21:00:5c:77:0f". Below it is the text "Enter a MAC address in the following format: xxxxxxxxxx:xxxxxx".
- A "Send" button.
- Text: "Wake all clients at once:
- Text: "Or Click the MAC address to wake up an individual device:"
- A table with columns "Interface", "MAC address", and "Description".
- A "Notes" section with the text: "This service can be used to wake up (power on) computers by sending special 'Magic Packets'. The NIC in the computer that is to be woken up must support Wake on LAN and has to be configured properly (WOL cable, BIOS settings)."

Siproxd

- 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
- siproxd
- Proxy server
- Antivirus
- VPN**
- IPsec
- OpenVPN
- PPTP
- L2TP
- Status**
- Captive Portal

siproxd: Settings

Settings **Users**

Inbound interface	WAN <input type="button" value="v"/> Select the inbound interface.
Outbound interface	WAN <input type="button" value="v"/> Select the outbound interface.
Listening port	<input type="text"/> Enter the port on which to listen for SIP traffic (default 5060). Do not change this unless you know what you're doing.
Enable RTP proxy	Enable <input type="button" value="v"/> Enable or disable the RTP proxy. (default is enabled)
RTP port range (lower)	<input type="text"/> Enter the bottom edge of the port range siproxd will allocate for incoming RTP traffic. This range must be one not blocked by the firewall (default 7070).
RTP port range (upper)	<input type="text"/> Enter the top edge of the port range siproxd will allocate for incoming RTP traffic. This range must be one not blocked by the firewall (default 7079).
RTP stream timeout	<input type="text"/> After this number of seconds, an RTP stream is considered dead and proxying it will be stopped (default 300sec).
Default expiration timeout	<input type="text"/> If a REGISTER request dose not contain an Expires header or expires= parameter, this number of seconds will be used and reported back to the UA in the answer.
Enable proxy authentication	<input type="checkbox"/> If this is checked, clients will be forced to authenticate themselves at the proxy (for registration only).
Outbound proxy hostname	<input type="text"/> Enter the hostname of an outbound proxy to send all traffic to. This is only useful if you have multiple masquerading firewalls to cross.
Outbound proxy port	<input type="text"/> Enter the port of the outbound proxy to send all traffic to. This is only useful if you have multiple masquerading firewalls to cross.
Expedited Forwarding	<input type="checkbox"/> This service is designed to allow ISPs to offer a service with attributes similar to a "leased line". This service offers the ULTIMATE IN LOW LOSS, LOW LATENCY AND LOW JITTER by ensuring that there is always sufficient room in output queues for the contracted expedited forwarding traffic.

Antivirus

- 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
- siproxd
- Proxy server
- Antivirus
- VPN**
- IPsec
- OpenVPN
- PPTP
- L2TP
- Status**
- Captive Portal

Antivirus: HTTP proxy (havp + clamav)

HTTP proxy **Files Scanner** **Settings**

Enable	<input type="checkbox"/> Check this for enable proxy.
Proxy mode	Standard <input type="button" value="v"/> Select interface mode: standard - client(s) bind to the 'proxy port' on selected interface(s); parent for squid - configure HAHP as parent for Squid proxy; transparent - all http requests on interface(s) will be translated to the HAHP proxy server without any client(s) additional configuration necessary (worked as 'parent for squid' with 'transparent' Squid proxy); internal - HAHP listen internal interface (127.0.0.1) on 'proxy port', use you own traffic forwarding rules.
Proxy interface(s)	none LAN <input type="button" value="v"/> The interface(s) for client connections to the proxy. Use ^Ctrl + L/Cli for multiple selection.
Proxy port	<input type="text"/> This is the port the proxy server will listen on (for example: 8080). This port must be different from Squid proxy.
Parent proxy	<input type="text"/> Enter the parent (upstream) proxy settings as PROXY:PORT format or leave empty.
Enable X-Forwarded-For	<input type="checkbox"/> If client sent this header, FORWARDED_IP setting defines the value, then it is passed on. You might want to keep this disabled for security reasons. Enable this if you use your own parent proxy after HAHP, so it will see the original client IP. Disabling this also disables Xac header generation.
Enable Forwarded IP	<input type="checkbox"/> If HAHP is used as parent proxy by some other proxy, this allows to write the real users IP to log, instead of proxy IP.
Language	Local <input type="button" value="v"/> Select the language in which the proxy server will display error messages to users.
Max download size, Bytes	<input type="text"/> Enter value (in Bytes) or leave empty. Downloads larger, than 'Max download size' will be blocked. Only if not whitelisted!
HTTP Range requests	<input type="checkbox"/> Set this for allow HTTP Range requests, and broken downloads can be resumed. Allowing HTTP Range is a security risk, because partial HTTP requests may not be properly scanned. Whitelisted sites are allowed to use Range in any case.
Whitelist	<input type="text"/>

spamD

The screenshot shows the SenseWebConfigurator interface. The top navigation bar includes the Sense logo and the text "webConfigurator". A left-hand menu lists various system and interface options. The main content area is titled "SpamD: External Sources" and contains sub-tabs for "SpamD Whitelist", "SpamD Settings", and "SpamD Database". Below these tabs is a table with columns for "Provider Name", "Provider Type", and "Description".

Proxy server

The screenshot shows the "Proxy server: General settings" configuration page. The left-hand menu is visible, and the main content area has tabs for "General", "Upstream Proxy", "Cache Mgmt", "Access Control", "Traffic Mgmt", "Auth Settings", and "Local Users". The "General" tab is active, displaying a list of settings:

- Proxy interface:** WAN (selected), LAN. Description: The interface(s) the proxy server will bind to.
- Allow users on interface:** . Description: If this field is checked, the users connected to the interface selected in the 'Proxy interface' field will be allowed to use the proxy, i.e., there will be no need to add the interface's subnet to the list of allowed subnets. This is just a shortcut.
- Transparent proxy:** . Description: If transparent mode is enabled, all requests for destination port 80 will be forwarded to the proxy server without any additional configuration necessary.
- Bypass proxy for Private Address Space (RFC 1918) destination:** . Description: Do not forward traffic to Private Address Space (RFC 1918) **destination** through the proxy server but directly through the firewall.
- Bypass proxy for these source IPs:** . Description: Do not forward traffic from these **source** IPs through the proxy server but directly through the firewall. Separate by semi-colons (;).
- Enabled logging:** . Description: This will enable the access log. Don't switch this on if you don't have much disk space left.
- Log store directory:** /var/squid/log. Description: The directory where the log will be stored (note: do not end with a / mark).
- Log rotate:** . Description: Defines how many days of logfiles will be kept. Rotation is disabled if left empty.
- Proxy port:** 3128. Description: This is the port the proxy server will listen on.
- ICP port:** . Description: This is the port the Proxy Server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.
- Visible hostname:** localhost. Description: This is the URL to be displayed in proxy server error messages.
- Administrator email:** admin@localhost. Description: This is the email address displayed in error messages to the users.
- Language:** English. Description: Select the language in which the proxy server will display error messages to users.

Proxy filter

The screenshot shows the Sense webConfigurator interface. The left sidebar contains a navigation menu with categories: System, Interfaces, Firewall, and Services. The main content area is titled "Proxy filter SquidGuard: General settings" and includes tabs for "General settings", "Default", "ACL", "Destinations", "Times", "Exceptions", and "Log". The "General settings" tab is active, showing several configuration options:

- Enable:** A checked checkbox. Below it, text reads: "Check this for enable squidGuard. For saving configuration YOU need click button 'Save' on bottom of page. After changing configuration squidGuard you must apply all changes." There is an "Apply" button and a status indicator "SquidGuard service state: STOPPED".
- Blacklist:** A checked checkbox. Below it, text reads: "Check this for enable blacklist".
- Blacklist proxy:** A text input field. Below it, text reads: "Blacklist upload proxy - enter here, or leave blank. Format: host[:port] login:pass. Default proxy port: 1080. Example: '192.168.0.1:8080 user:pass'".
- Blacklist URL:** A text input field containing "http://www45.indowebster.com/5ecb97166960461dee7bd5dc0da904b0.rar". Below it, text reads: "Enter FTP, HTTP or LOCAL (pfSense) URL blacklist archive, or leave blank." There are "Upload list" and "Restore list" buttons.
- View GUI log:** An unchecked checkbox. Below it, text reads: "Check this for view GUI log".

A "Save" button is located at the bottom of the configuration area.

- VPN :
- IPsec
 - Open VPN
 - PPTP
 - L2TP

IPsec

The screenshot shows the Sense webConfigurator interface for "VPN: IPsec: Mobile". The left sidebar is the same as in the previous screenshot. The main content area is titled "VPN: IPsec: Mobile" and includes tabs for "Tunnels", "Mobile clients", "Pre-shared keys", and "CA's". The "Mobile clients" tab is active, showing a configuration page for mobile clients. At the top, a red banner with a warning icon states: "The changes have been applied successfully. You can also [cancel](#) the filter reload progress." Below this, there are several configuration options:

- Allow mobile clients:** A checked checkbox.
- Phase 1 proposal (Authentication):** A red header for the following options:
 - Negotiation mode:** A dropdown menu set to "aggressive". Below it, text reads: "Aggressive is faster, but less secure."
 - My identifier:** A text input field set to "My IP address".
 - Encryption algorithm:** A dropdown menu set to "3DES". Below it, text reads: "Must match the setting chosen on the remote side."
 - Hash algorithm:** A dropdown menu set to "SHA1". Below it, text reads: "Must match the setting chosen on the remote side."
 - Diffie-hellman group:** A dropdown menu set to "2". Below it, text reads: "X = 769, Y = 769, Z = 1629, S = 1529. Must match the setting chosen on the remote side."
 - NAT Traversal:** An unchecked checkbox. Below it, text reads: "Enable NAT Traversal (NAT-T). Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls."
 - DPD Interval:** A text input field set to "120". Below it, text reads: "Dead Peer Detection interval in seconds. Leave this empty to only respond to DPD requests and not send any requests."
 - Lifetime:** A text input field set to "1200" with "seconds" next to it.
 - Authentication method:** A dropdown menu set to "Pre-shared key". Below it, text reads: "Must match the setting chosen on the remote side."
 - Certificate:** A text input field.

Open VPN

- Advanced
- Firmware
- General Setup
- Package
- 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
- spproxy
- Proxy server
- Antivirus
- VPN**
- IPsec
- OpenVPN
- PPTP
- L2TP
- Status**
- Captive Portal

OpenVPN: Server

Server
Client
Client Specific Overrides

General information

Disabled	<input type="checkbox"/> Disable this server Set this option to disable this server without removing it from the list.
Server Mode	Peer to Peer (SSL/TLS)
Protocol	UDP
Interface	wan1
Local port	1194
Description	<input type="text"/> <small>You may enter a description here for your reference (not parsed).</small>

Cryptographic Settings

TLS Authentication	<input checked="" type="checkbox"/> Enable authentication of TLS packets. <input checked="" type="checkbox"/> Automatically generate a shared TLS authentication key.
Peer Certificate Authority	ca
Server Certificate	server
DH Parameters Length	3024 bits
Encryption algorithm	AES-256-GCM (256 bit)

Tunnel Settings

Tunnel Network	<input type="text"/> <small>This is the virtual network used for private communications between this server and client hosts expressed using CIDR (eg. 10.0.0.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients. (see Address Pool)</small>
Redirect Gateway	<input type="checkbox"/> Force all client generated traffic through the tunnel.
Local Network	<input type="text"/> <small>This is the network that will be accessible from the remote endpoint. Expressed as a CIDR range. You may leave this blank if you don't want to add a route to the local network through the tunnel on the remote machine. This is generally set to your LAN network.</small>

PPTP

- Advanced
- Firmware
- General Setup
- Package
- 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
- spproxy
- Proxy server
- Antivirus
- VPN**
- IPsec
- OpenVPN
- PPTP
- L2TP
- Status**
- Captive Portal

VPN: VPN PPTP

Configuration
Users

off

Redirect incoming PPTP connections to:

PPTP redirection
Enter the IP address of a host which will accept incoming PPTP connections.

Enable PPTP server

Server address
Enter the IP address the PPTP server should use on its side for all clients.

Remote address range
Specify the starting address for the client IP subnet.

Subnet netmask
Hint: 24 is 255.255.255.0

No. PPTP users
Hint: 10 is TEN pptp clients

PPTP DNS Servers
primary and secondary DNS servers assigned to PPTP clients

RADIUS issued IP

WDS Server

RADIUS

Use a RADIUS server for authentication
When set, all users will be authenticated using the RADIUS server specified below. The local user database will not be used.

Enable RADIUS accounting
Send accounting packets to the RADIUS server.

Secondary RADIUS server for fallback authentication
When set, all requests will go to the secondary server when primary fails

RADIUS NAS IP

RADIUS Accounting Update

- 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

The screenshot shows the Sense webConfigurator interface. The top navigation bar includes the Sense logo, 'webConfigurator', and a user profile 'maria.kr.india.com'. A sidebar on the left lists system settings: System, Advanced, Firmware, General Setup, Packages, Setup wizard, Static routes, and Interfaces. The main content area displays 'Status: Captive portal (1)' and a table with the following data:

IP address	MAC address	Username	Session start
192.168.1.20	00:22:64:4a:10:16	sys	01/14/2010 21:31:58

Below the table is a 'Show last activity' button.

CARP(failover)

The screenshot shows the Sense webConfigurator interface for CARP status. The top navigation bar includes the Sense logo, 'webConfigurator', and a user profile 'maria.kr.india.com'. The sidebar on the left lists system settings: System, Advanced, Firmware, General Setup, Packages, Setup Wizard, Routing, Cert Manager, and User Manager. The main content area displays 'Status: CARP' and a table with the following data:

Carp Interface	Virtual IP	Status
Could not locate any defined CARP interfaces.		

DHCP leases

The screenshot shows the Sense webConfigurator interface. The top navigation bar includes the Sense logo, the title "webConfigurator", and a notification "DHCP leases started". A sidebar on the left lists menu items: System (Advanced, Firmware, General Setup, Packages, Setup Wizard, Static routes), Interfaces (assign), and WAN. The main content area is titled "Diagnostics: DHCP leases" and contains a table with the following data:

IP address	MAC address	Hostname	Start	End	Online	Lease Type
192.168.1.20	00:22:64:4a:10:18	user-dc66a6e3	2010/01/14 20:52:36	2010/01/14 22:52:36	online	active

Below the table is a button labeled "Show all configured leases".

Filter reload

The screenshot shows the Sense webConfigurator interface. The top navigation bar includes the Sense logo, the title "webConfigurator", and the URL "maria.prindia.com". A sidebar on the left lists menu items: System (Advanced, Firmware, General Setup, Packages, Setup Wizard, Routing). The main content area is titled "Status: Filter Reload Status" and displays a yellow message box: "Done. The filter rules have been reloaded." Below this is a section for "Queue Status".

Interfaces

The screenshot shows the Sense webConfigurator interface. The top navigation bar includes the Sense logo, the title "webConfigurator", and a notification "making your WAN keys... WAN is now started". A sidebar on the left lists menu items: System (Advanced, Firmware, General Setup, Packages, Setup Wizard, Static routes), Interfaces (assign), WAN, LAN, Firewall (Aliases, NAT, Rules, Schedules, Traffic Shaper, Virtual IPs), Services (Captive portal, DNS forwarder, DHCP relay, DHCP server, Dynamic DNS, Load Balancer, OLSR, PPPoE Server, RIP, SNMP, UPnP, OpenNTPD, Wake on LAN, spond, Antivirus, SpamD, Proxy server, Proxy filter), and VPN (Psec, OpenVPN). The main content area is titled "Status: Interfaces" and displays details for two interfaces:

WAN interface (w0)

Status	up
MAC address	00:0f:ea:08:ae:08
IP address	10.252.108.7
Subnet mask	255.255.255.0
Gateway	10.252.108.1
ISP DNS servers	192.168.2.1
Media	100baseTX <full-duplex>
In/out packets	8316583266 (74.47 MB/10.26 MB)
In/out errors	0/0
Collisions	0

LAN interface (r0)

Status	up
MAC address	00:80:1c:2c:13:0a
IP address	192.168.1.5
Subnet mask	255.255.255.0
Media	100baseTX <full-duplex>
In/out packets	6121485033 (10.63 MB/79.27 MB)
In/out errors	0/0
Collisions	0

Using dial-on-demand will bring the connection up again if any packet triggers it. To substantiate this point: disconnecting manually will **not** prevent dial-on-demand from making connections to the outside! Don't use dial-on-demand if you want to make sure that the line is kept disconnected.

Note: In/out counters will wrap at 32bit (4 Gigabyte) !

IPsec

The screenshot shows the Sense webConfigurator interface. The top navigation bar includes the Sense logo, the text 'webConfigurator', and the URL 'maria.pr.indika.com'. A left-hand menu lists various system settings. The main content area is titled 'Status: IPsec' and features tabs for 'Overview', 'SA0', and 'SP0'. Below the tabs is a table with columns for 'Local IP', 'Remote IP', 'Local Network', 'Remote Network', 'Description', and 'Status'. A note below the table states: 'Note: You can configure your IPsec here.'

Load balancer

The screenshot shows the Sense webConfigurator interface for the Load Balancer section. The top navigation bar includes the Sense logo, the text 'webConfigurator', and the URL 'maria.pr.indika.com'. A left-hand menu lists various system settings. The main content area is titled 'Status: Load Balancer; Pool' and features a 'Pools' tab with a sub-tab for 'Virtual Servers'. Below the tabs is a table with columns for 'Name', 'Type', 'Gateways', 'Status', and 'Description'.

Packages logs

The screenshot shows the Sense webConfigurator interface for the Package logs section. The top navigation bar includes the Sense logo, the text 'webConfigurator', and the URL 'maria.pr.indika.com'. A left-hand menu lists various system settings. The main content area is titled 'Diagnostics: Package logs' and features a 'spamd' tab. Below the tab is a table with the header 'Last 50 spamd log entries'. The table contains two columns: a timestamp and a log message. The messages are all 'last message repeated 10 times' or 'last message repeated 2 times'.

Last 50 spamd log entries	
Jan 14 13:31:12	last message repeated 2 times
Jan 14 13:41:12	last message repeated 10 times
Jan 14 13:51:12	last message repeated 10 times
Jan 14 14:01:12	last message repeated 10 times
Jan 14 14:11:12	last message repeated 10 times
Jan 14 14:21:12	last message repeated 10 times
Jan 14 14:31:12	last message repeated 10 times
Jan 14 14:41:13	last message repeated 10 times
Jan 14 14:51:13	last message repeated 10 times
Jan 14 15:01:13	last message repeated 10 times
Jan 14 15:11:13	last message repeated 10 times
Jan 14 15:21:18	last message repeated 10 times
Jan 14 15:31:18	last message repeated 10 times
Jan 14 15:41:18	last message repeated 10 times
Jan 14 15:51:18	last message repeated 10 times
Jan 14 16:01:18	last message repeated 10 times
Jan 14 16:11:18	last message repeated 10 times
Jan 14 16:21:18	last message repeated 10 times
Jan 14 16:31:18	last message repeated 10 times
Jan 14 16:41:18	last message repeated 10 times
Jan 14 16:51:18	last message repeated 10 times
Jan 14 17:01:18	last message repeated 10 times
Jan 14 17:11:18	last message repeated 10 times
Jan 14 17:21:18	last message repeated 10 times

Queues

Sense webConfigurator maria.arindika.com

Status: Traffic shaper: Queues

Queue **Statistics**

Note:
Queue graphs take 5 seconds to sample data.
You can configure the Traffic Shaper here.

RRD Graphs

Status: RRD Graphs

System Traffic Packets Quality Queues QueueDrops Wireless Settings

Note: Change of color and/or style may not take effect until the next refresh

Graphs: Processor Style: Inverse

maria.arindika.com - System :: Processor - 4 hours - 1 minute average

utilization, number

user nice system interrupt processes

	minimum	average	maximum	current
User util.	0.00	254.10	3.16	1.50
Nice util.	0.00	240.77	800.00	0.00
System util.	0.00	582.55	5.54	1.02
Interrupt	0.00	11.16	476.11	476.11
Processes	30.00	38.56	57.70	55.00

Dec 27 02:18:11 2009

maria.arindika.com - System :: Processor - 16 hours - 1 minute average

utilization, number

Services

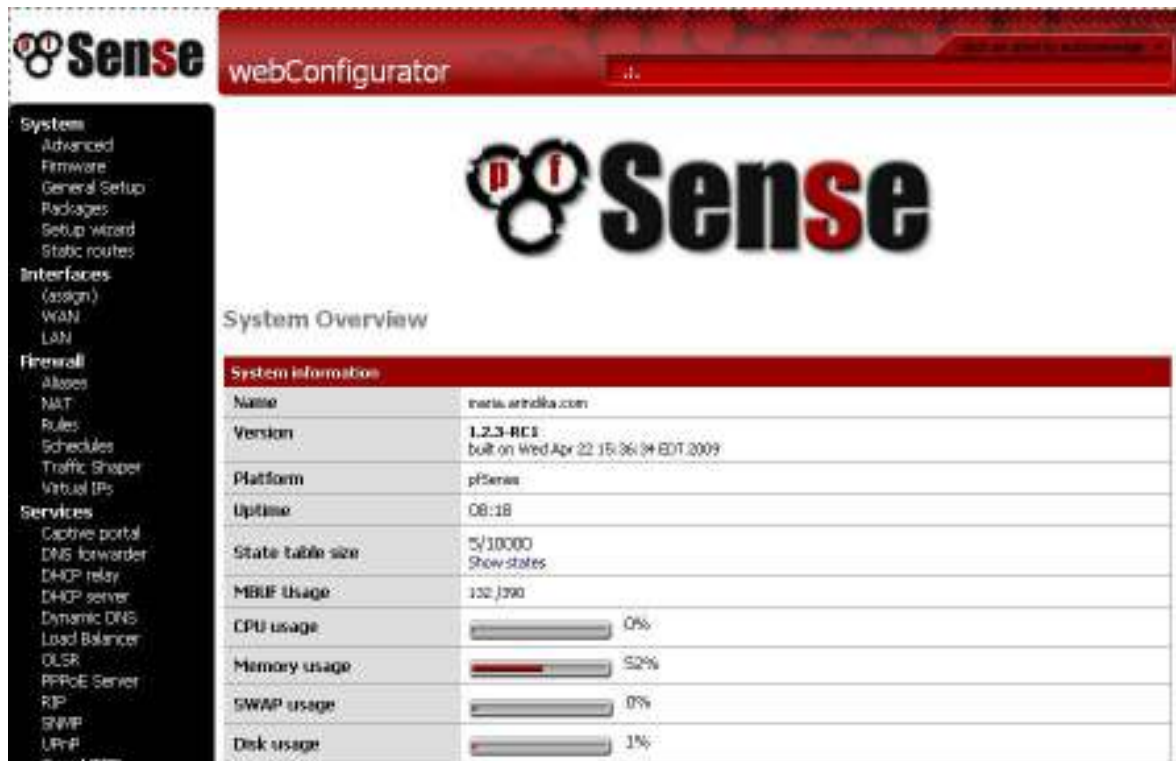


The screenshot shows the 'Services' page in the Sense webConfigurator. The interface includes a navigation menu on the left with categories like System, Interfaces, Firewall, and Services. The main content area displays a table of services with their status and control icons.

Status: Services





Service	Description	Status
sproxd	Proxy for handling NAT of multiple SIP devices to a single public IP.	Stopped
hntp	Antivirus HTTP proxy Service	Running
spsnd	Targets like spsnd are fake SMTP servers, which accept connections but don't deliver mail. Instead, they keep the connections open and reply very slowly. If the peer is patient enough to actually complete the SMTP dialogue (which will take ten minutes or more), the target returns a 'temporary error' code (4xx), which indicates that the mail could not be delivered successfully and that the sender should keep the mail in their queue and retry again later.	Running
epid	Proxy server Service	Running
epidGuard	Proxy server filter Service	Stopped
dnsmasq	DNS Forwarder	Running
ntpd	NTP clock sync	Running
lighttpd	Captive Portal	Running
dhcpd	DHCP Service	Running

System



The screenshot shows the 'System Overview' page in the Sense webConfigurator. The page features the Sense logo and a table of system information.

System Overview

System Information	
Name	travis.atholka.com
Version	1.2.3-RC1 built on Wed Apr 22 15:36:04 EDT 2009
Platform	pSeries
Uptime	08:18
State table size	5/10000 Show states
MBUF Usage	132 / 390
CPU usage	 0%
Memory usage	 52%
SWAP usage	 0%
Disk usage	 1%

System logs

- 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
- OpenNTFD
- Wake on LAN
- spoofed
- Proxy server
- Antivirus
- VPN
- IPsec
- OpenVPN
- PPPoE
- L2TP
- Status
- Captive Portal

Status: System logs: System

System	Firewall	DHCP	Portals Auth	IPsec VPN	PPPoE VPN	Load Balancer	OpenVPN	OpenNTFD	Settings
Last 50 system log entries									
Dec 27 01:28:21	routed[48967]	static route 192.168.182.1/32 -> 127.0.0.2	impossibly lacks ip						
Dec 27 01:28:21	routed[48967]	static route 192.168.182.1/32 -> 127.0.0.2	impossibly lacks ip						
Dec 27 01:33:20	routed[48967]	static route 192.168.182.1/32 -> 127.0.0.2	impossibly lacks ip						
Dec 27 01:33:20	routed[48967]	static route 192.168.182.1/32 -> 127.0.0.2	impossibly lacks ip						
Dec 27 01:38:19	routed[48967]	static route 192.168.182.1/32 -> 127.0.0.2	impossibly lacks ip						
Dec 27 01:38:19	routed[48967]	static route 192.168.182.1/32 -> 127.0.0.2	impossibly lacks ip						
Dec 27 01:49:17	routed[48967]	static route 192.168.182.1/32 -> 127.0.0.2	impossibly lacks ip						
Dec 27 01:49:17	last message repeated 2 times								
Dec 27 01:59:16	routed[48967]	static route 192.168.182.1/32 -> 127.0.0.2	impossibly lacks ip						
Dec 27 01:59:16	routed[48967]	static route 192.168.182.1/32 -> 127.0.0.2	impossibly lacks ip						
Dec 27 01:59:15	last message repeated 2 times								
Dec 27 02:00:01	php: Resuming configuration for all packages.								
Dec 27 02:00:02	php: Reloading Squid for configuration sync.								
Dec 27 02:00:02	php: The command 'usr/local/sbin/squid -k reconfigure' returned exit code '1', the output was '2009/12/27 02:00:02 parseConfigFile: squid.conf:60 unrecognized: 'delay_class' 2009/12/27 02:00:02 parseConfigFile: squid.conf:61 unrecognized: 'delay_class' 2009/12/27 02:00:02 parseConfigFile: squid.conf:62 unrecognized: 'delay_parameters' 2009/12/27 02:00:02 parseConfigFile: squid.conf:63 unrecognized: 'delay_initial_bucket_level' 2009/12/27 02:00:02 parseConfigFile: squid.conf:64 unrecognized: 'delay_access' squid: ERROR: No running copy'								
Dec 27 02:00:02	php: The command 'chgrp -R -x http:usr/local/share/examples/http/templates_ex' returned exit code '1', the output was 'chgrp: (usr/local/share/examples/http/templates_ex): No such file or directory'								
Dec 27 02:00:02	php: The command 'chown -R -x http:usr/local/share/examples/http/templates_ex' returned exit code '1', the output was 'chown: (usr/local/share/examples/http/templates_ex): No such file or directory'								
Dec 27 02:00:02	php: Stopping HTTP.								
Dec 27 02:00:03	php: Reloading Squid for configuration sync.								
Dec 27 02:00:03	php: The command 'usr/local/sbin/squid -k reconfigure' returned exit code '1', the output was '2009/12/27 02:00:03 parseConfigFile: squid.conf:60 unrecognized: 'delay_class' 2009/12/27 02:00:03 parseConfigFile: squid.conf:61 unrecognized: 'delay_class' 2009/12/27 02:00:03 parseConfigFile: squid.conf:62 unrecognized: 'delay_parameters' 2009/12/27 02:00:03 parseConfigFile: squid.conf:63 unrecognized: 'delay_initial_bucket_level' 2009/12/27 02:00:03 parseConfigFile: squid.conf:64 unrecognized: 'delay_access' squid: ERROR: No running copy'								
Dec 27 02:00:03	squid[9562]: Squid Parent: child process 10058 started.								
Dec 27 02:00:04	check_reload_status: check_reload_status is starting.								
Dec 27 02:00:04	dmesd[9495]: Not supported data format.								

Traffic graph

- 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

Status: Traffic Graph

Interface: WAN

Note: the Adobe SVG Viewer, Firefox 1.5 or later or other browser supporting SVG is required to view the graph.

In 0 Kbps 12/27/2009 02:23:10 [Switch to bytes/s](#) WAN
Out 0 Kbps [AutoScale \(up\)](#)
 Graph shows last 360 seconds

75 Kbps

50 Kbps

25 Kbps

UPnP

The screenshot shows the MikroTik WinBox webConfigurator interface. The top header includes the 'Sense' logo, 'webConfigurator', and the URL 'mikrotik.com'. A left-hand navigation menu lists various system settings. The main content area displays the 'Status: UPnP Status' page, which indicates that 'UPnP is currently disabled'.

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

Arp table

The screenshot shows the MikroTik WinBox webConfigurator interface with the 'Diagnostics: ARP Table' page selected. A table displays the current ARP entries.

IP address	MAC address	Hostname	Interface
192.168.182.10	00:21:00:5c:77:d3	user-dc:66a5e63	LAN

Backup/restore

Diagnostics: Backup/restore

Backup configuration

Click this button to download the system configuration in XML format.

Backup area:

Do not backup package information.

Encrypt this configuration file.

Do not backup RRD data (NOTE: RRD Data can consume ++ megabytes of config.xml space!)

Download configuration

Restore configuration

Open a configuration XML file and click the button below to restore the configuration.

Restore area:

Configuration file is encrypted.

Restore configuration

Note:
The firewall may need a reboot after restoring the configuration.

Reinstall packages

Click this button to reinstall all system packages. This may take a while.

Reinstall packages

Command prompt

Sense webConfigurator mikrotik.com

Diagnostics: Execute command

Note: this function is unsupported, use it on your own risk!

Execute shell command

Command:

Download

File to download:

Upload

File to upload:

PHP Execute

Command:

Example: `interfaces_cfg_configure()`

Edit file

The screenshot shows the pfSense webConfigurator interface. The top header includes the pfSense logo and the text 'webConfigurator'. A navigation menu on the left lists various system settings categories such as System, Interfaces, Firewall, and Services. The main content area is titled 'Diagnostics: Edit File' and features a 'Save/Load from path:' input field with 'Load' and 'Save' buttons. Below this is a large, empty text area for editing the file content.

Factory defaults

The screenshot shows the pfSense webConfigurator interface for the 'Diagnostics: Factory defaults' page. The top header includes the pfSense logo and the text 'webConfigurator'. The left navigation menu is visible. The main content area is titled 'Diagnostics: Factory defaults' and contains a warning message: 'If you click "Yes", the firewall will:'. Below this, a list of actions is provided: 'Reset to factory defaults', 'LAN IP address will be reset to 192.168.1.1', 'System will be configured as a DHCP server on the default LAN interface', 'Reboot after changes are installed', 'WAN interface will be set to obtain an address automatically from a DHCP server', 'webConfigurator admin username will be reset to "admin"', and 'webConfigurator admin password will be reset to "pfSense"'. At the bottom, a confirmation question 'Are you sure you want to proceed?' is followed by 'Yes' and 'No' buttons.

Halt system

Sense webConfigurator maria.arnoldka.com

System
Advanced
Firmware
General Setup
Packages
Setup Wizard
Routing

Diagnostics: Halt system

Are you sure you want to halt the system?

Ping

Sense webConfigurator click as used to acknowledge

System
Advanced
Firmware
General Setup
Packages
Setup wizard
Static routes

Interfaces
(assign)
WAN
LAN

Firewall
Aliases
NAT
Rules
Schedules
Traffic Shaper
Virtual IPs

Services
Captive portal
DNS forwarder
DHCP relay

Diagnostics: Ping

Host:

Interface:

Count:

Ping output:

```
PING 192.168.1.5 <192.168.1.5> from 192.168.1.5: 56 data bytes
64 bytes from 192.168.1.5: icmp_seq=0 ttl=64 time=0.236 ms
64 bytes from 192.168.1.5: icmp_seq=1 ttl=64 time=0.868 ms
64 bytes from 192.168.1.5: icmp_seq=2 ttl=64 time=0.846 ms

--- 192.168.1.5 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.846/0.114/0.236/0.886 ms
```

Note: Multi-wan is not supported from this utility currently.

Reboot system

Sense webConfigurator maria.arnoldka.com

System
Advanced
Firmware
General Setup
Packages
Setup Wizard
Routing

Diagnostics: Reboot System

Are you sure you want to reboot the system?

Routes

- Advanced
- Firmware
- General Setup
- Package
- Setup Wizard
- Routing
- Cart 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
- Open/PTD
- Wake on LAN
- speed
- Proxy server
- Arbitrator
- VPN**
- IPsec
- OpenVPN
- PPTP
- L2TP

Diagnostics: Routing tables

Name resolution Enable
Enable this to attempt to resolve names when displaying the tables.

Note: By enabling name resolution, the query should take a bit longer. You can stop it at any time by clicking the Stop button in your browser.

IPv4							
Destination	Gateway	Flags	Refs	Use	MTU	Netif	Expire
127.0.0.1	127.0.0.1	UH	0	5647	16384	lo	
192.168.182.0/24	br#1	UC	0	0	1500	eth	
192.168.182.1	127.0.0.2	USHG	0	5645	16384	lo	
192.168.182.10	00:21:00:5c:77:0f	UHLW	1	5199	1500	eth	795

IPv6							
Destination	Gateway	Flags	Refs	Use	MTU	Netif	Expire
:::	:::	UHL	1	0	16384	lo	
fe80::%v0%64	br#1	UC	0	0	1500	eth	
fe80::2e0:1d7:fe3c:130a%v0	00:e0:1c:3c:13:0a	UHL	1	0	1500	lo	
fe80::%v0%64	br#2	UC	0	0	1500	veth	
fe80::207:ea7:fe09:ae08%v0	00:0f:ea:09:ae:08	UHL	1	0	1500	lo	
fe80::%v0%64	fe80::1%v0	U	0	0	16384	lo	
fe80::1%v0	br#1	UHL	1	0	16384	lo	
f01::1%32	br#1	UC	0	0	1500	eth	
f01::2%32	br#2	UC	0	0	1500	veth	
f01::4%32	:::	UC	0	0	16384	lo	
f02::%v0%32	br#1	UC	0	0	1500	eth	
f02::%v0%32	br#2	UC	0	0	1500	veth	
f02::%v0%32	:::	UC	0	0	16384	lo	

states

- System**
- Advanced
- Firmware
- General Setup
- Package
- Setup wizard
- Static routes
- Interfaces**
- (assign)
- WAN
- LAN
- Firewall**
- Aliases
- NAT
- Rules
- Schedules
- Traffic Shaper
- Virtual IPs
- Services**

Sense webConfigurator v2.10.0 (2014-08-08)

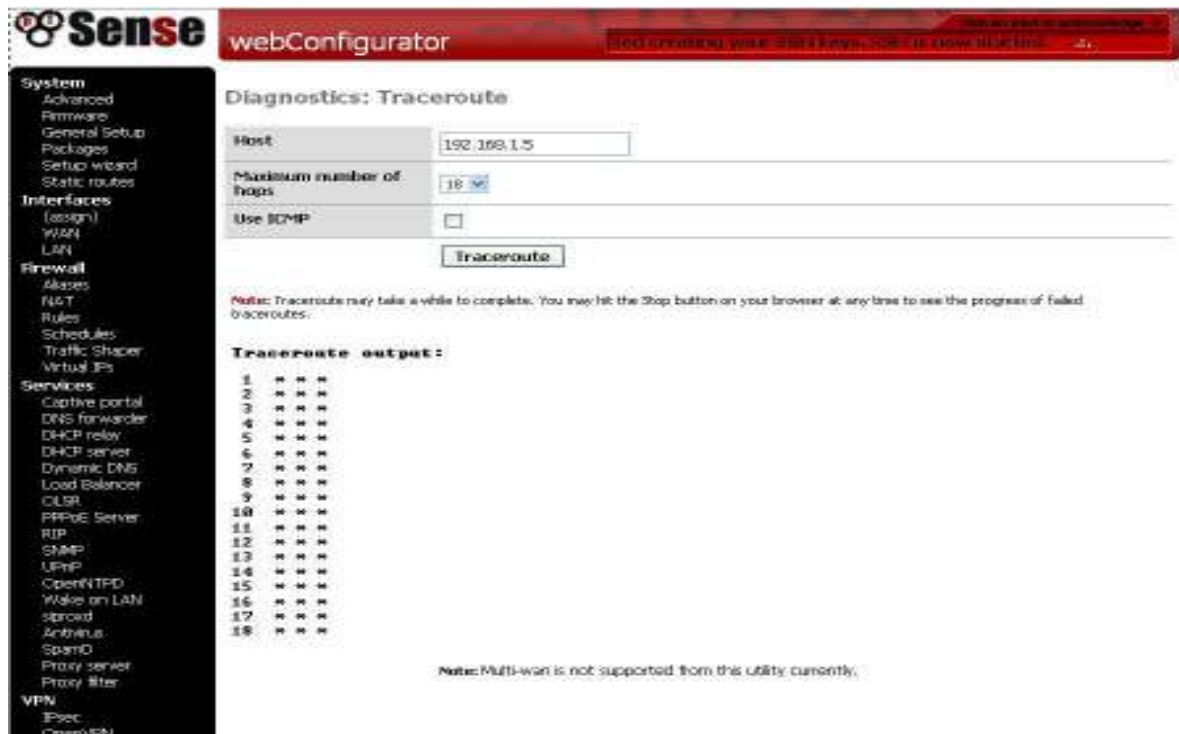
Diagnostics: Show States

States

Current data rows: 5 Filter expression:

Proto	Source -> Router -> Destination	State
udp	192.168.1.5:53 <- 192.168.1.20:1025	MULTIPLE: MULTIPLE
tcp	192.168.1.5:80 <- 192.168.1.20:3549	FIN_WAIT_2: FIN_WAIT_2
tcp	192.168.1.5:80 <- 192.168.1.20:3550	FIN_WAIT_2: FIN_WAIT_2
tcp	192.168.1.5:80 <- 192.168.1.20:3551	FIN_WAIT_2: FIN_WAIT_2
tcp	192.168.1.5:80 <- 192.168.1.20:3552	ESTABLISHED: ESTABLISHED

Traceroute



Sense webConfigurator Help | Settings | Logout | [Home](#)

Diagnostics: Traceroute

Host:

Maximum number of hops:

Use ICMP:

Note: Traceroute may take a while to complete. You may hit the Stop button on your browser at any time to see the progress of failed traceroutes.

Traceroute output:

```

1  * * * *
2  * * * *
3  * * * *
4  * * * *
5  * * * *
6  * * * *
7  * * * *
8  * * * *
9  * * * *
10 * * * *
11 * * * *
12 * * * *
13 * * * *
14 * * * *
15 * * * *
16 * * * *
17 * * * *
18 * * * *

```

Note: Multi-wan is not supported from this utility currently.

Packet capture



Sense webConfigurator Help | Settings | Logout | [Home](#)

Diagnostics: Packet Capture

Packet capture

Interface:

Host Address:
This value is either the Source or Destination IP address. The packet capture will look for this address in either field. This value can be a domain name or IP address. If you leave this field blank, all packets on the specified interface will be captured.

Port:
The port can be either the source or destination port. The packet capture will look for this port in either field. Leave blank if you do not want to capture to filter by port.

Packet Length:
The Packet length is the number of bytes the packet will capture for each payload. Default value is 1500. This value should be the same as the MTU of the Interface selected above.

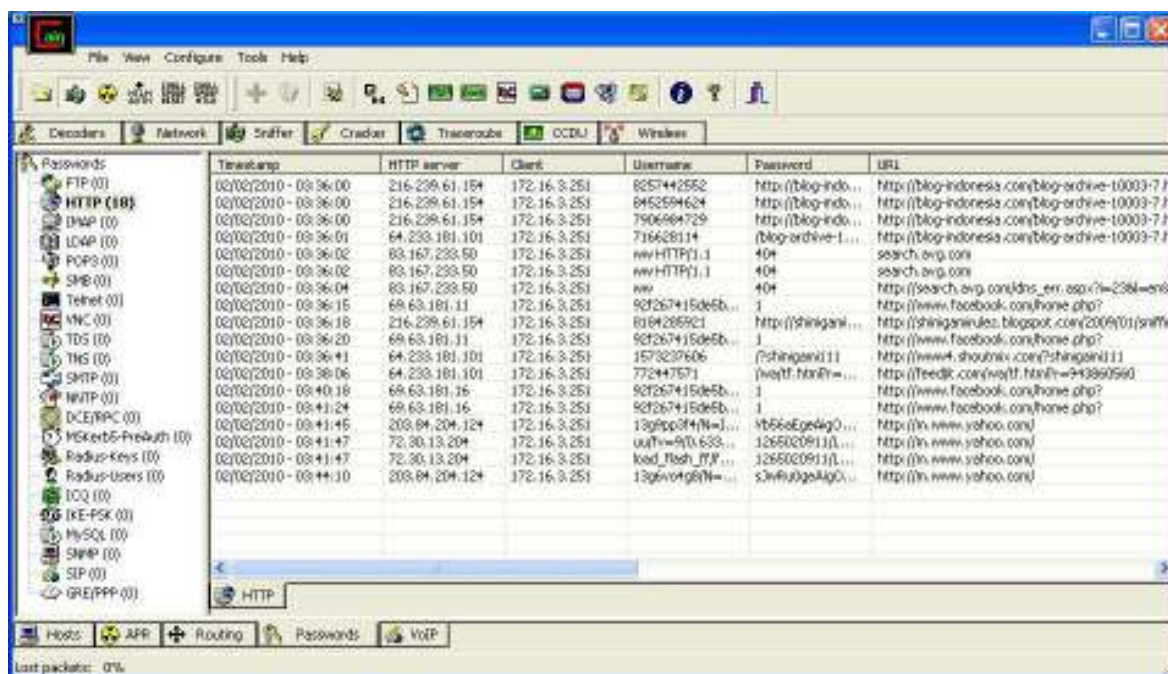
Count:
This is the number of packets the packet capture will grab. Default value is 100. Enter 0 (zero) for no count limit.

Level of Detail:
This is the level of detail that will be displayed after hitting 'Stop' when the packets have been captured. Note: This option does not affect the level of detail when downloading the packet capture.

Reverse DNS Lookup:
This check box will cause the packet capture to perform a reverse DNS lookup associated with all IP addresses. Note: This option can be CPU intensive for large packet captures.

Packet Capture is running.

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



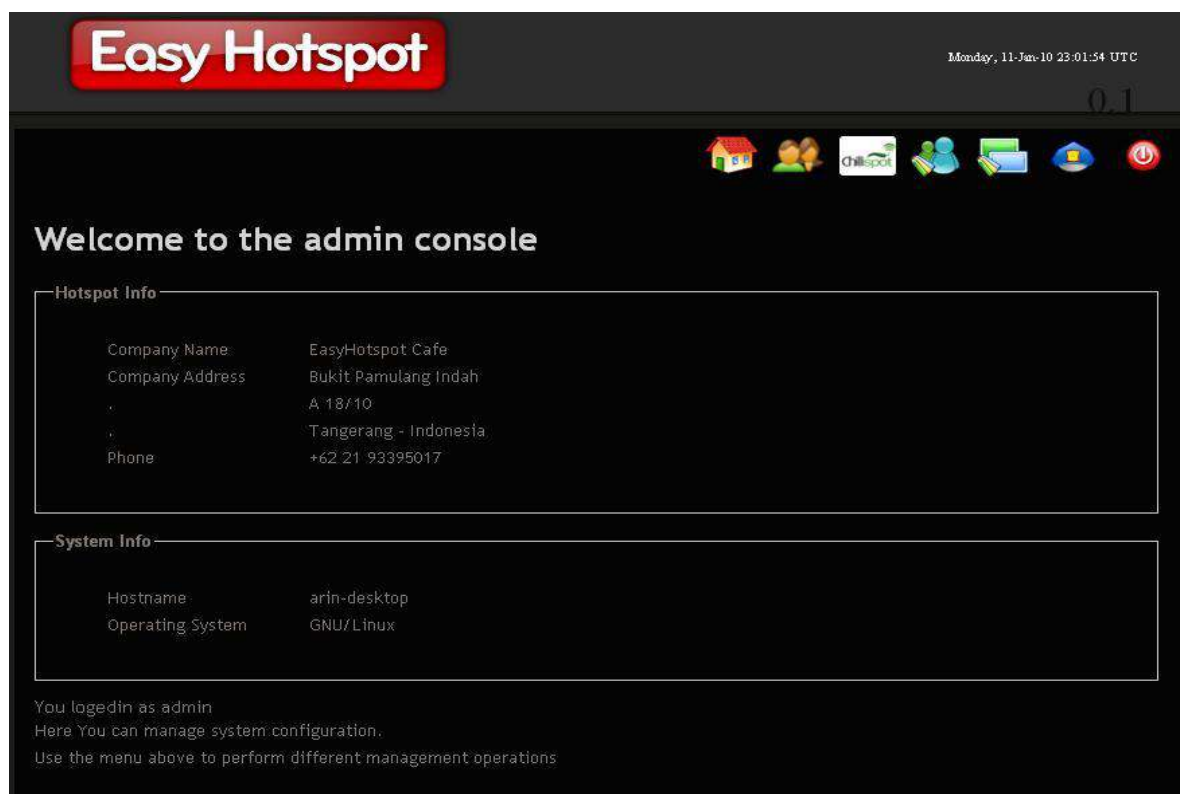
3.1 Easy Hotspot

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

Login admin



Tampilan Menu admin



Postpaid account

Easy Hotspot Tuesday, 12-Jan-10 00:01:05 UTC

Postpaid Account Management

Realname	Username	Password	Used	Bill by	Current Total	Action
yanti	yanti	qwe.	94	time	18,723	
Tanta	quro	quro123	0	time	0	
eee	eeeeeee	eee	0	time	0	
eqeee	eeeeee	ee.	0	time	0	
ee	eqqqq	e	0	time	0	
ewew	eqq	e	0	time	0	
we	we	e	0	time	0	
w	w	w	0	packet	0	
Testing Acc	test	testing	0	time	0	

Name:
 Username:
 Password:
 Bill by:

Voucher account

Easy Hotspot Tuesday, 12-Jan-10 00:01:07 UTC

Voucher Management

Username	Password	Billing Plan	Time Used	Time Remain	Packet Used	Packet Remain	Printed
nukviy7	cilgonup	1 jam	---	---	---	---	no
nolneb14	cudbabet	1 jam	---	---	---	---	no
dixwob6	mutpupul	1 jam	---	---	---	---	no
netvov7	togkubeb	1 jam	---	---	---	---	no
motkab5	sopmanak	1 jam	---	---	---	---	no
nuvboz5	barlodop	1 jam	---	---	---	---	no
selvow10	tibpegac	1 jam	---	---	---	---	no
zarxul8	bitsobob	1 jam	---	---	---	---	no
bonnor10	galrubim	1 jam	---	---	---	---	no
nuwduk10	kurbopad	1 jam	---	---	---	---	no








1 2 3 > Last >

Number of voucher:
 Billing Plan:











Invoice management

Easy Hotspot Tuesday, 12-Jan-10 00:01:10 UTC

0.1








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 statistic

Easy Hotspot Tuesday, 12-Jan-10 00:01:12 UTC

0.1

Hotspot Statistics


Voucher Created

Vouchers Info

Vouchers Created	116
Used	1
Expired	0

Billing Plans

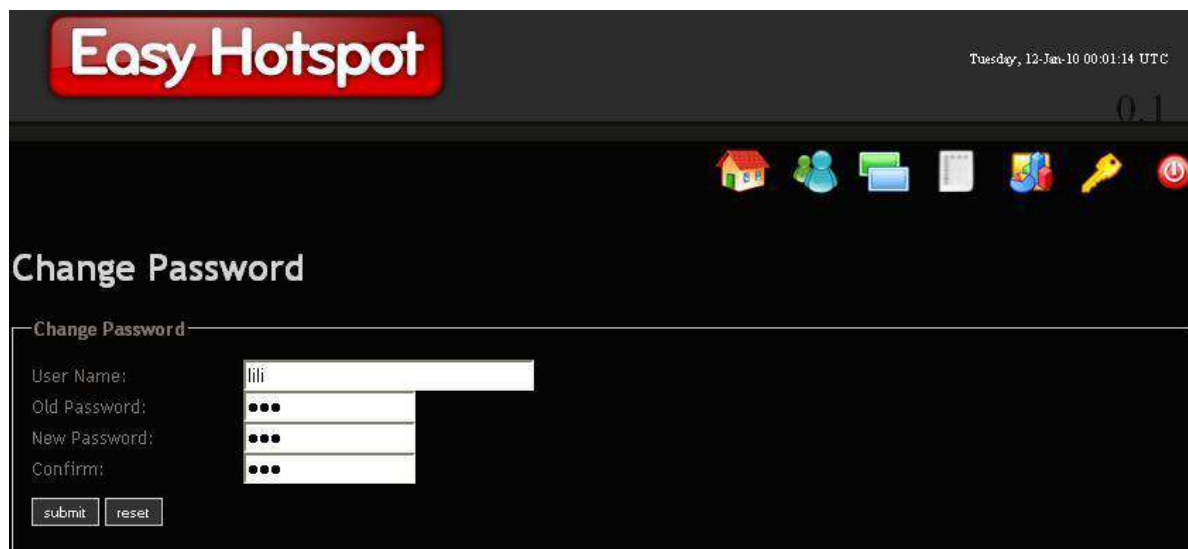
1 jam	112
20 Mega	4



Postpaid Account Info

Account Created	9
Used	2

Change password



The screenshot shows the 'Easy Hotspot' web interface. At the top left is the 'Easy Hotspot' logo in a red rounded rectangle. At the top right, the date and time are displayed as 'Tuesday, 12-Jan-10 00:01:14 UTC' and the version '0.1'. Below the header is a navigation bar with icons for home, user profile, settings, help, and power. The main content area is titled 'Change Password' and contains a form with the following fields: 'User Name:' with the value 'lili', 'Old Password:', 'New Password:', and 'Confirm:'. Each password field is masked with dots. At the bottom of the form are 'submit' and 'reset' buttons.

Login kasir



The screenshot shows the 'Easy Hotspot' login page. At the top is the 'Easy Hotspot' logo in a red rounded rectangle. Below the logo, the text 'Watchout it's hot!' and 'Easyhotspot 0.1' is displayed. The login form consists of two input fields: 'User Name:' with the value 'vcool' and 'Password:' which is masked with dots. A large 'Login' button is positioned below the password field. At the bottom of the page, the text 'EasyHotspot - Hotspot Management System' and 'GNU Public License' is visible.

Menu kasir

Easy Hotspot Tuesday, 12-Jan-10 00:01:17 UTC 0.1

Welcome to EasyHotspot System

Hotspot Info

- Company Name: EasyHotspot Cafe
- Company Address: Bukit Pamulang Indah
A.18/10
Tangerang - Indonesia
- Phone: +62 21 93395017

System Info

- Hostname: arin-desktop
- Operating System: GNU/Linux

You logged in as vcool

Postpaid account kasir

Easy Hotspot Tuesday, 12-Jan-10 00:01:19 UTC 0.1

Postpaid Account Management

Realname	Username	Password	Used	Bill by	Current Total	Action
yanti	yanti	qwe	94	time	18,723	
Tanta	quro	quro123	0	time	0	
eee	eeeeeee	eee	0	time	0	
eqeee	eeeeee	ee	0	time	0	
ee	eqqqq	e	0	time	0	
ewew	eqq	e	0	time	0	
we	we	e	0	time	0	
w	w	w	0	packet	0	
Testing Acc	test	testing	0	time	0	

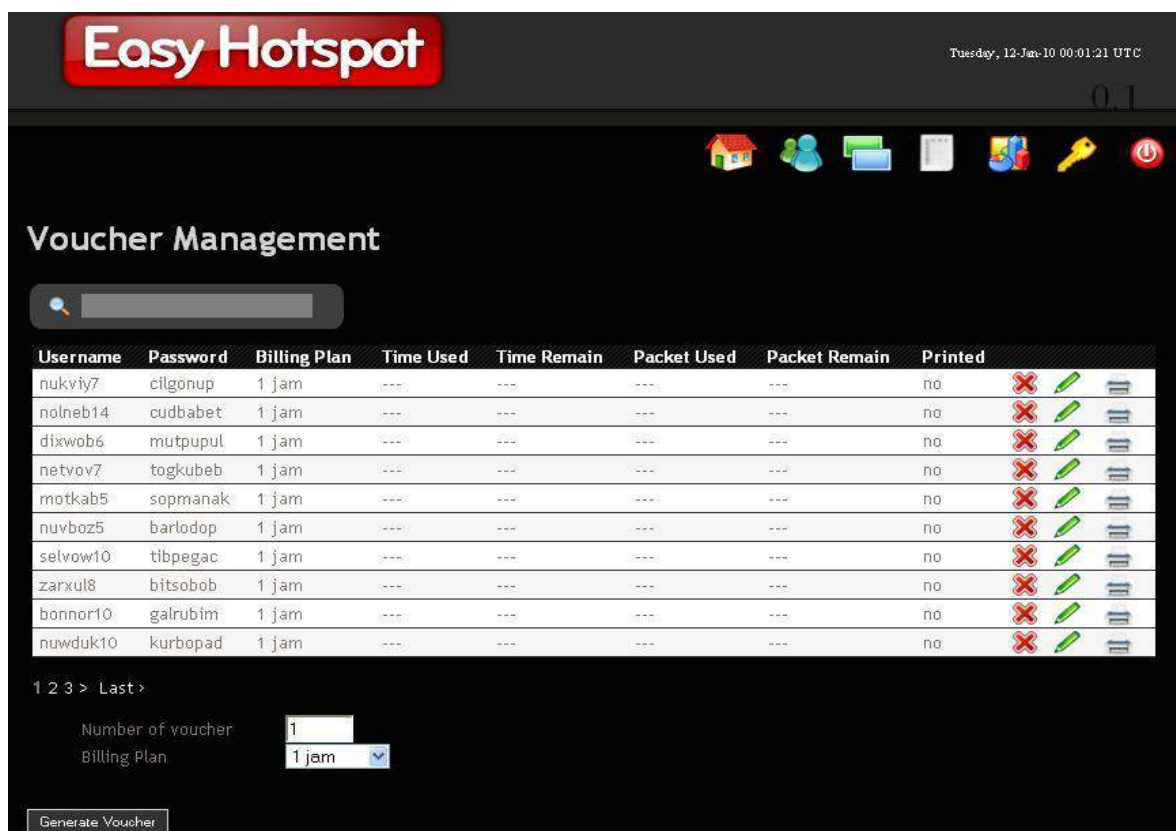
Name:

Username:

Password:

Bill by:

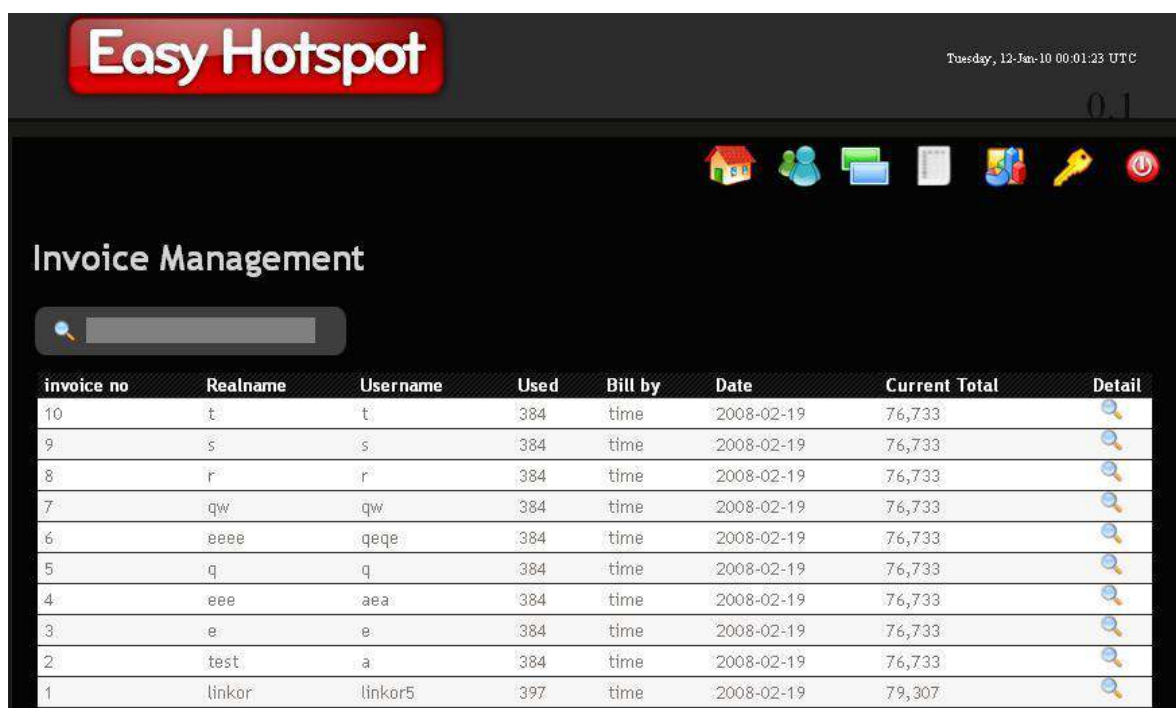
Voucher kasir



The screenshot shows the 'Voucher Management' section of the Easy Hotspot web interface. At the top, there is a search bar. Below it is a table with columns: Username, Password, Billing Plan, Time Used, Time Remain, Packet Used, Packet Remain, and Printed. The table lists ten vouchers, all with a '1 jam' billing plan and 'no' printed status. To the right of each row are three icons: a red 'X', a green pencil, and a printer icon. Below the table, there are navigation links '1 2 3 > Last >', a form for 'Number of voucher' (set to 1) and 'Billing Plan' (set to 1 jam), and a 'Generate Voucher' button.

Username	Password	Billing Plan	Time Used	Time Remain	Packet Used	Packet Remain	Printed
nukviy7	cilgonup	1 jam	---	---	---	---	no
nolneb14	cudbabet	1 jam	---	---	---	---	no
dixwob6	mutpupul	1 jam	---	---	---	---	no
netvov7	togkubeb	1 jam	---	---	---	---	no
motkab5	sopmanak	1 jam	---	---	---	---	no
nuvboz5	bartodop	1 jam	---	---	---	---	no
selvow10	tibpegac	1 jam	---	---	---	---	no
zarxul8	bitsobob	1 jam	---	---	---	---	no
bonnor10	galrubim	1 jam	---	---	---	---	no
nuwduk10	kurbopad	1 jam	---	---	---	---	no

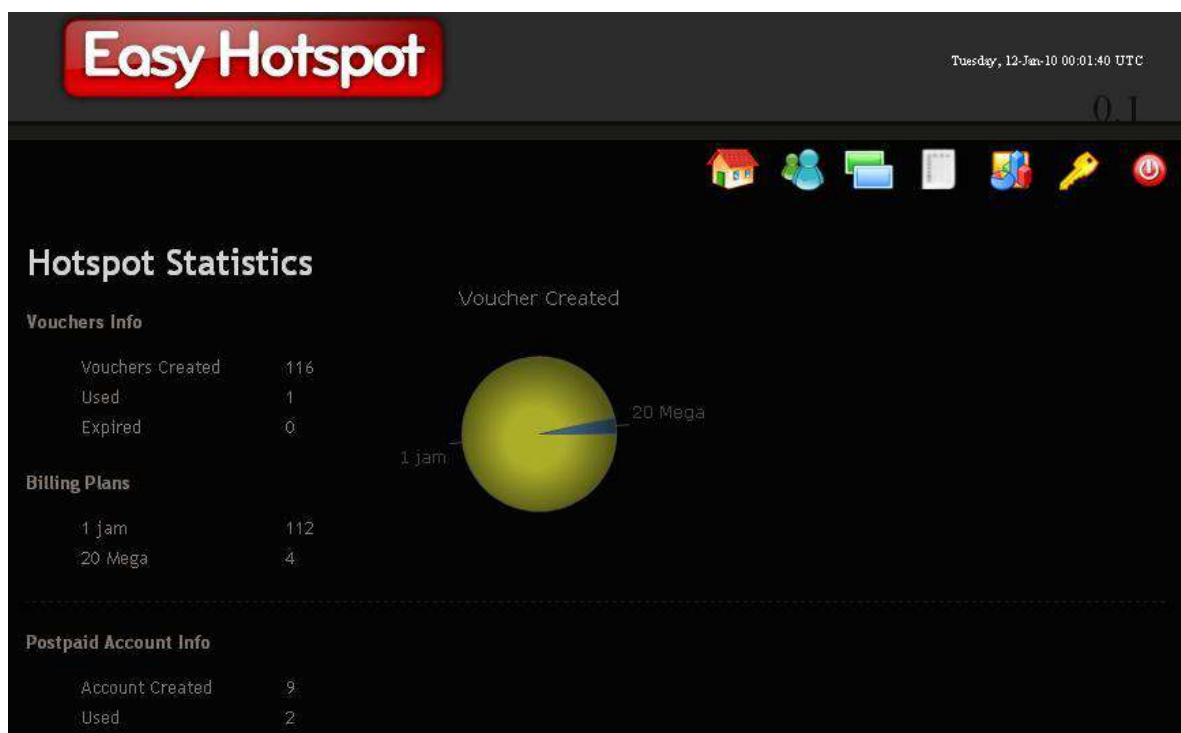
Pembuatan Invoice pada kasir



The screenshot shows the 'Invoice Management' section of the Easy Hotspot web interface. It features a search bar and a table with columns: invoice no, Realname, Username, Used, Bill by, Date, Current Total, and Detail. The table lists ten invoices, all with a 'time' bill by type and a 'Current Total' of 76,733, except for invoice 1 which has a total of 79,307. Each row has a magnifying glass icon in the 'Detail' column.

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 statistic kasar



Change password kasar

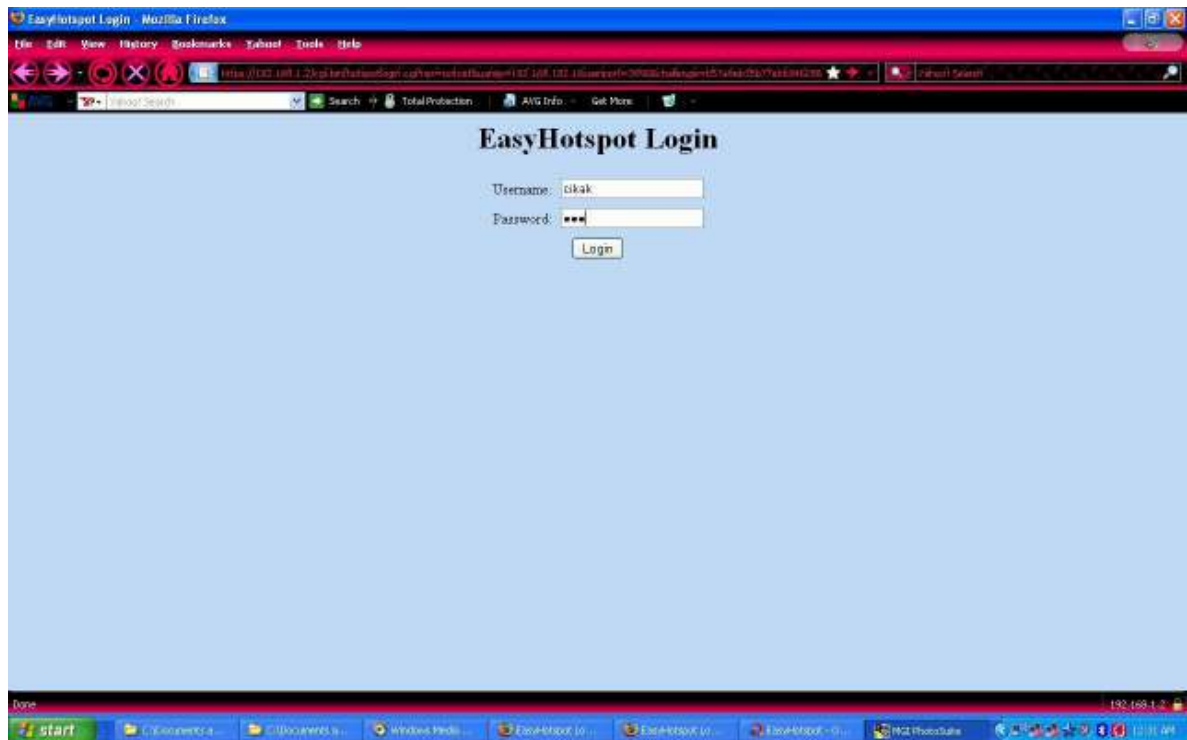
The screenshot displays the Easy Hotspot dashboard with the 'Change Password' form. The header and navigation bar are identical to the previous screenshot. The main content area is titled 'Change Password' and contains a form with the following fields:

- Change Password** (form title)
- User Name:**
- Old Password:**
- New Password:**
- Confirm:**

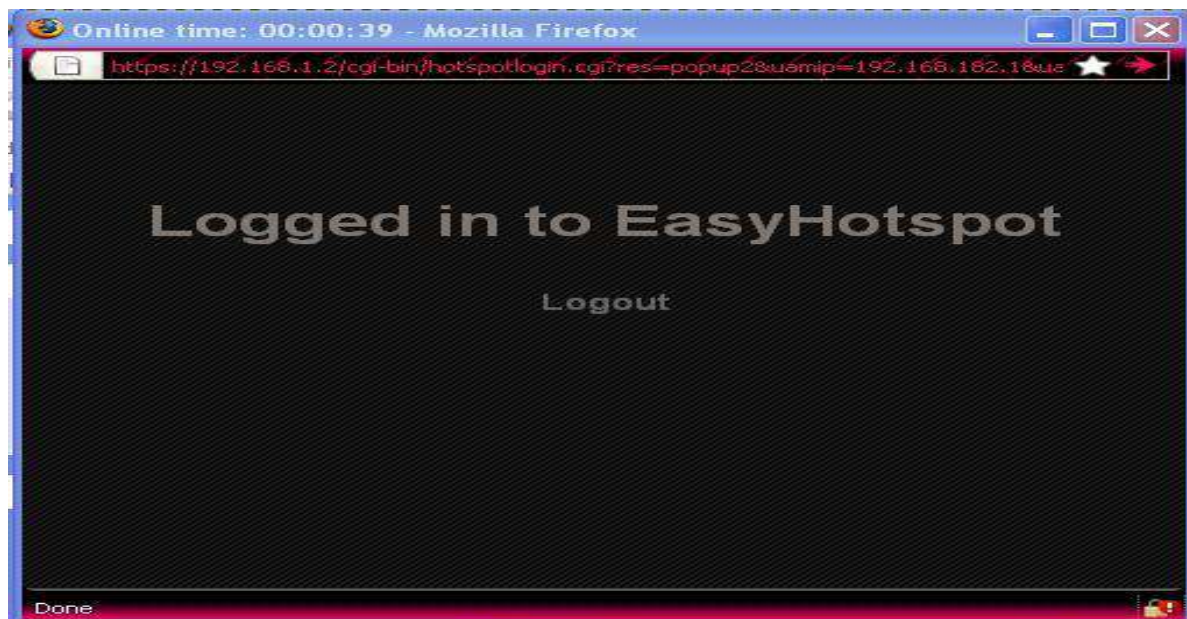
At the bottom of the form are two buttons: 'submit' and 'reset'.

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

Login easyhotspot



Logout easyhotspot



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

