WLAN oder LAN Gastnetz einrichten mit einem Captive Portal (Hotspot Funktion)

aqui (Level 5) - Jetzt verbinden

06.07.2008, aktualisiert 24.02.2015, 447058 Aufrufe, 283 Kommentare, 24 Danke

Dieses Tutorial gibt einen kurzen Leitfaden für ein hier im Forum sehr häufig angefragtes Netzdesign zur sicheren Integration eines Gäste oder Besucher WLANs oder LANs.
Es beschreibt die einfache und preiswerte Installation eines sogenannten *"Captive Portals"* (Hotspot Funktion) für einen unabhängigen WLAN und / oder LAN Gastzugang in Firmen, Hotels, Cafes und anderen Lokationen, die eine automatische, Web Browser basierende Authentisierung mit einem Benutzernamen oder Einmal-Passwörtern (Vouchers) sowie eine Überwachung des Zugangs ermöglicht.

Inhaltsverzeichnis

Allgemeine Einleitung

Als Basis für das Captive Portal kommt hier die frei verfügbare Software pfSense oder OpnSense zum Einsatz, die über ein einfaches und intuitives Websetup diese Funktion zur Verfügung stellt.
(Für M0n0wall als weitere Alternative wurde kürzlich der Support eingestellt, so das diese Option hier nur noch nebenbei Erwähnung findet)
Die pfSense Firewall hat darüberhinaus weitergehende Features wie einen OpenVPN_Server, Timeserver, Clustering, Dual WAN Port usw. sie steht kommerziellen Firewalls in nichts nach !
Zudem kann sie über ein kleines ALIX Mini Mainboard in eine handliche 3 Port Appliance verbaut werden. Solch ein fertiges Set ist bei diversen Anbietern wie z.B. *Varia Store* erhältlich.
Das Tutorial geht nicht im Detail auf alle Features von pfSense und seiner Router- und Firewall Funktionen ein. Diese sind aber recht einfach und intuitiv und können über ein einfaches Webinterface per Mausklick bedient werden, was auch für Firewall Anfänger sehr einfach zu handhaben ist.
Die einfache Installationsprozedur kann detailiert HIER hier nachgelesen werden.
Es genügt ein (alter) vorhandener PC mit 2 (optional 3 oder mehr) Netzwerkkarten und einem CD ROM Laufwerk.
Eine Festplatte ist nicht zwingend erforderlich, denn pfSense bootet bequem von einer CD oder einem USB Stick sofern ein USB Port vorhanden ist !
Es empfiehlt sich in jedem Falle einen FAT32 formatierten (Standard) USB Memory Stick in einen der PC USB Ports **vor** dem Booten der CD zu

stecken. Dieser speichert dann automatisch die Konfiguration ab, die ja sonst nach einem Reboot mit reinem CD Betrieb verloren ist.
Mehr oder minder ist diese Option heutzutage aber irrelevant, denn fast niemand mehr bootet ein solches System von einer CD es sei denn der verwendete PC ist wirklich alt.
Kann direkt vom USB Stick gebootet werden kann das CD ROM Laufwerk vollständig entfallen.
Mit einem einfachen CD oder USB Stick Setup ist ein schneller problemloser Aufbau und Test der Firewall Funktion und des Gäste Captive Portals ohne großen Aufwand möglich für denjenigen der sich nur mal einen Überblick verschaffen will !
Ein alter PC oder ein altes Mainboard aus der Bastelkiste kann so sinnvoll *recycelt* werden sieht man von den Stromkosten ab...

Für einen späteren und dauerhaften Betrieb sollte man aber in jedem Falle eine verschleissfreie CF (Compact Flash) Flash Speicherkarte als *Festplatte* verwenden oder einen bootbaren USB Stick oder....
Noch besser und energetisch sinnvoller: gleich eine feste Appliance mit einem ALIX Mini Mainboard verwenden, aber dazu später mehr...
Der simple Grund dafür ist das dort keine beweglichen Teile mehr vorhanden sind, die im Dauerbetrieb einen Ausfall durch Verschleiss verursachen können !
So hat diese Firewall Hardware keinerlei weitere bewegliche Teile mehr und ist für den Dauerbetrieb bestens gerüstet !

Bei einer PC basierten Lösung steckt man als verschleissfreien Festplattenersatz einen preiswerten IDE / CF Flashkartenadapter wie z.B. DIESEN hier oder DIESEN(klick) direkt in den normalen PC IDE Festplattenport auf dem Mainboard statt des 40 oder 80 poligen Festplattenkabels.
Wie so etwas dann im Betrieb aussieht kann man HIER ansehen.
Die Flashkarte sollte nicht kleiner als 512 MB sein.
So lassen sich z.B. ungenutzte, zu klein gewordene CF Flashkarten aus der Digitalfotografie problemlos einer neuen und sinnvollen Verwendung zuführen.
Für modernere SATA Ports gibt es ebenfalls entsprechende Adapter oder man verwendet eine alte, ausgesonderte, zu klein gewordene SSD.

Dieser Adapter mit CF Karte fungiert dann in der Firewall wie eine normale Festplatte von der die pfSense dann bootet und arbeitet.
Natürlich kann man auch von einem USB Stick booten, was aber oft ein etwas moderneres Mainbord BIOS erfordert, das das Booten vom USB Stick supporten muss.
Der CF Adapter hat hier den großen Vorteil das er unter jeden Umständen in Uralt Mainboards, funktioniert durch die Universialität der parallelen IDE/ATA Festplatten Schnittstelle die in älterer Hardware immer vorhanden ist und unabhängig von USB Boot Features ist !!
Ferner ist er intern im Gehäuse durch äußere Manipulation geschützt im Gegensatz zu einem externen USB Stick !
Bei alter PC Hardware sollte mindestens 512 MB RAM onboard sein.

Wie eine CF Flashkarte oder USB Stick mit *physdiskwrite* "betankt" wird beschreibt das hiesige pfSense Forumstutorial für ALIX Boards im Detail:
Preiswerte, VPN fähige Firewall im Eigenbau oder als Fertiggerät

Nach der Installation auf der CF Karte oder USB_Stick bootet pfSense direkt davon und ist nach dem Einschalten sofort einsatzbereit.

Technisch besser: Feste Gehäuselösung (Appliance) statt alter PC

Ein gravierender Nachteil bei Betrieb der Firewall auf einer alten PC Hardware sind die laufenden Betriebskosten (Strom), Abwärme, Lüftergeräusche, Verschleiss und Platzbedarf.
Technisch sinnvoller und effektiver ist es das Captive Portal bzw. pfSense als schicke, kleine embedded Appliance statt auf einem klobigen PC zu verwenden. Die Gehäusegröße und der Stromverbrauch entspricht dem aktueller Router oder Firewalls. Die anfallenden Stromkosten reduzieren sich damit auf ca. 15-20 Euro im Jahr und alle anderen Nachteile entfallen ebenfalls.

Da die Mehrzahl der heutigen Installatonen auf diesen Boards beruhen ist der Aufbau oder auch die Verwendung eines Fertiggeräts auf Basis der beliebten ALIX 2D13 oder APU1D (Gig.Netzwerkports) Mini Mainboards in einem separaten Forumstutorial hier bei Administrator.de beschrieben, das auch für Laien und Anfänger sehr leicht umzusetzen ist:
Preiswerte, VPN fähige Firewall im Eigenbau oder als Fertiggerät

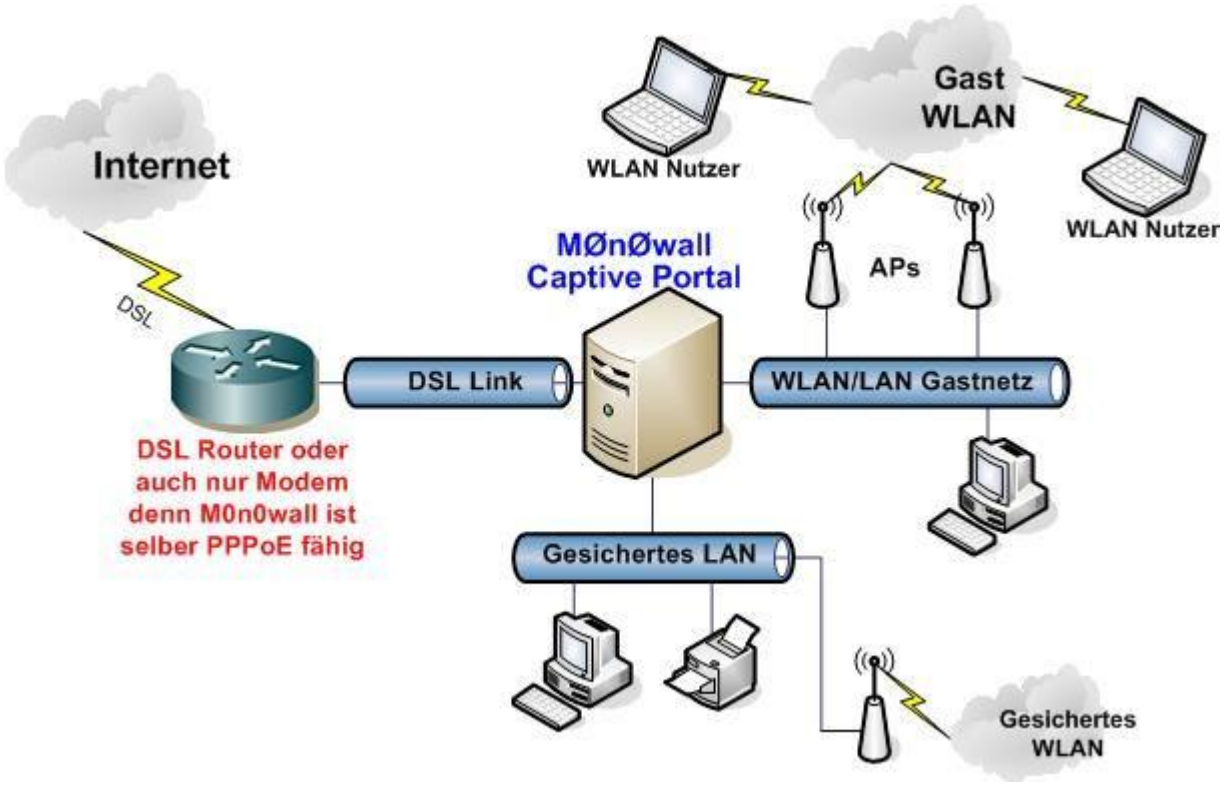
Download der pfSense Software

Wer dennoch bei der PC Plattfom bleiben möchte oder einen Uralt PC sinnvoll recyceln will findet ein ISO CD Image zum Brennen der Boot- und Installations CD und auch das CF/USB Flashkarten Image hier zum Download:
http://www.pfsense.org/index.php?option=com_content&task=view&i ... ("Here on the Mirrors" klicken)
Die pfSense "nanobsd" Images sind ausschliesslich für embedded Boards wie ALIX oder Soekris gedacht. Die Ziffer im Dateinamen gibt an für welche CF Flashkartengröße das Image gedacht ist.
Für den Betrieb auf alten PCs oder Atom Minibords wird das normale "RELEASE-i386" Image verwendet, was man auch per USB Stick oder CF

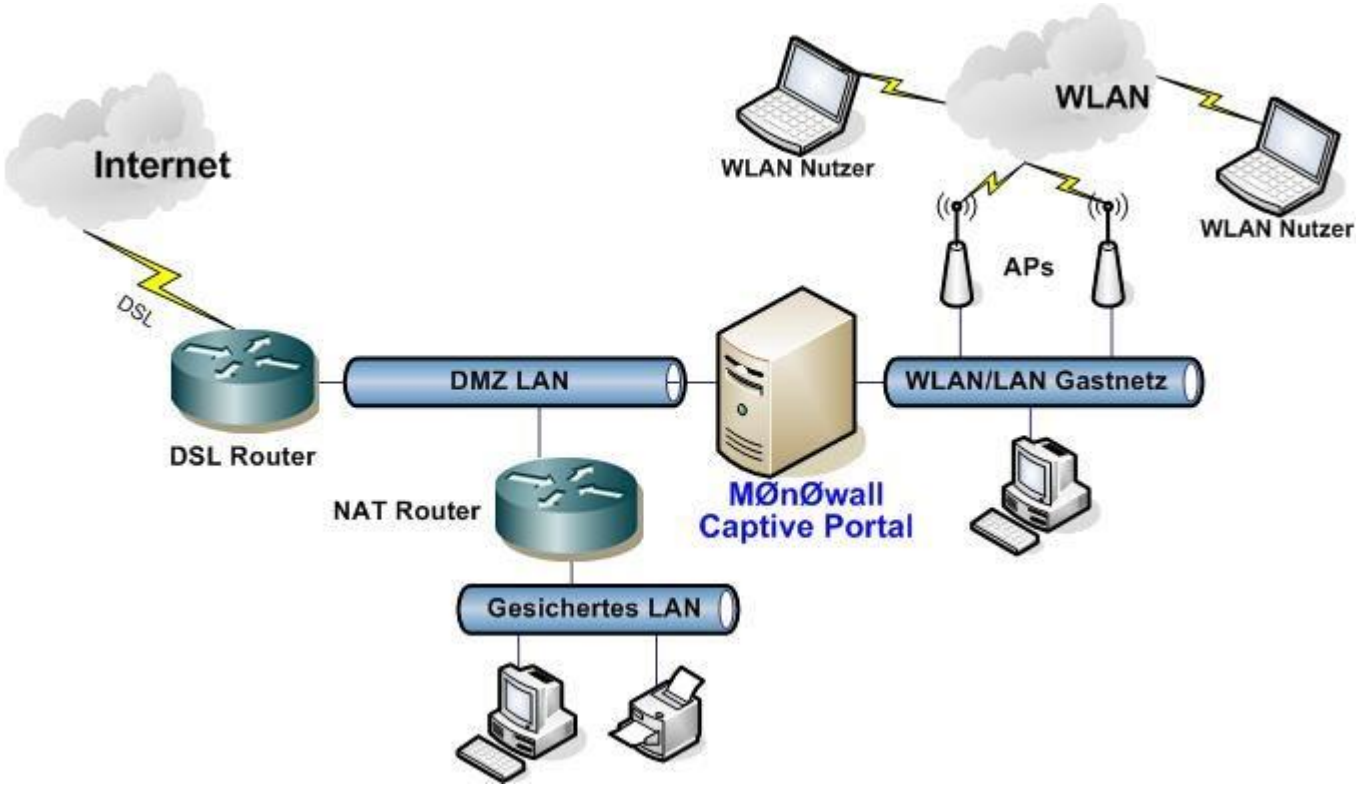
Flash bootet.

Neuerdings sogar ebenfalls ein VmWare Image zum Starten in einer VM mit dem kostenlosen VmWare_Player
Ein grafisches Windows Programm zum Beschreiben von CF Flashkarten in einem Kartenadapter ist der bekannte Win32DiskImager !
Generell sollte man aus Sicherheits- und Stabilitätsgründen aber immer, wenn irgend möglich, von der Installation einer Firewall in einer VM aus Sicherheitsgründen absehen !

Ein klassisches Netzdesign mit 3 Interfaces in der pfSense, sprich einem abgesicherten Verwaltungs- bzw. Firmennetz getrennt vom Gastzugang sähe so aus:



Da die pfSense direkt das PPPoE Protokoll unterstützt ist ein Router für einen Internet Zugang nicht zwingend erforderlich !
Ein einfaches DSL "nur Modem", (wie das einfache DSL Modem im o.a. ALIX Tutorial) oder ein Router der via "PPPoE Passthrough" Option in den reinen Modem Betrieb konfiguriert wurde, würde ebenfalls vollkommen reichen. (Siehe Schemazeichnung unten im Menüpunkt *Betrieb* !).
Es erspart späterer Probleme mit doppeltem NAT oder Performanceeinbußen in Router Kaskaden.
Achtung: Die Provider Zugangsdaten sind dann immer im Setup der Firewall (WAN Port, PPPoE Modus) einzugeben !
Ein Design mit einem zusätzlichen NAT Router ist aber ebenso problemlos und wird im folgenden Abschnitt zur Installation näher beschrieben.



Wer statt dedizierter WLAN Accesspoints überzählige WLAN Router als "nur" APs im Hotspot Netz verwenden will, findet HIER in der Alternative-3 eine genaue Anleitung wie diese für einen Betrieb als einfacher, "nur" WLAN Accesspoint zu konfigurieren sind !

Installation und Integration der Firewall ins Netzwerk

Nach dem Booten, egal ob per CD oder Flash Karte, ist pfSense sofort einsatzbereit. Als Default ist auf dem LAN Segment ein DHCP Server aktiv und entsprechende Regeln schon voreingestellt. Es reicht also hier einfach einen Laptop/PC anzuschliessen und loszulegen mit der Konfiguration.
Auf dem WAN / Internet Port ist im Default ein DHCP Client aktiv, der sich von einem vorhandenen DSL-Router mit aktivem DSL Anschluss automatisch eine IP, Gateway und DNS Adresse holt wenn man den WAN Port dort anschliesst.
Bei den recht bekannten ALIX Boards ist der WAN / Internet Port in der Regel immer der mittlere der 3 Ports.
Das LAN Segment arbeitet per Default auf dem IP Netz **192.168.1.0**.
Das Websetup zur Konfiguration des Systems hat die IP Adresse **192.168.1.1** und kann sofort mit dem Browser (IE oder Firefox etc.) unter **http://192.168.1.1** erreicht werden.
Der Konfigurationszugang hat die default Benutzer/Passwortkennung **admin** mit dem Passwort **pfsense** !

ACHTUNG: Wer andere IP Adressen bzw. Netze im LAN Segment hat oder das Portal in ein bestehendes LAN/WAN Umfeld integrieren will oder muss, kann die entsprechenden IP Einstellungen dafür natürlich **vorher** auf seine Belange einstellen.

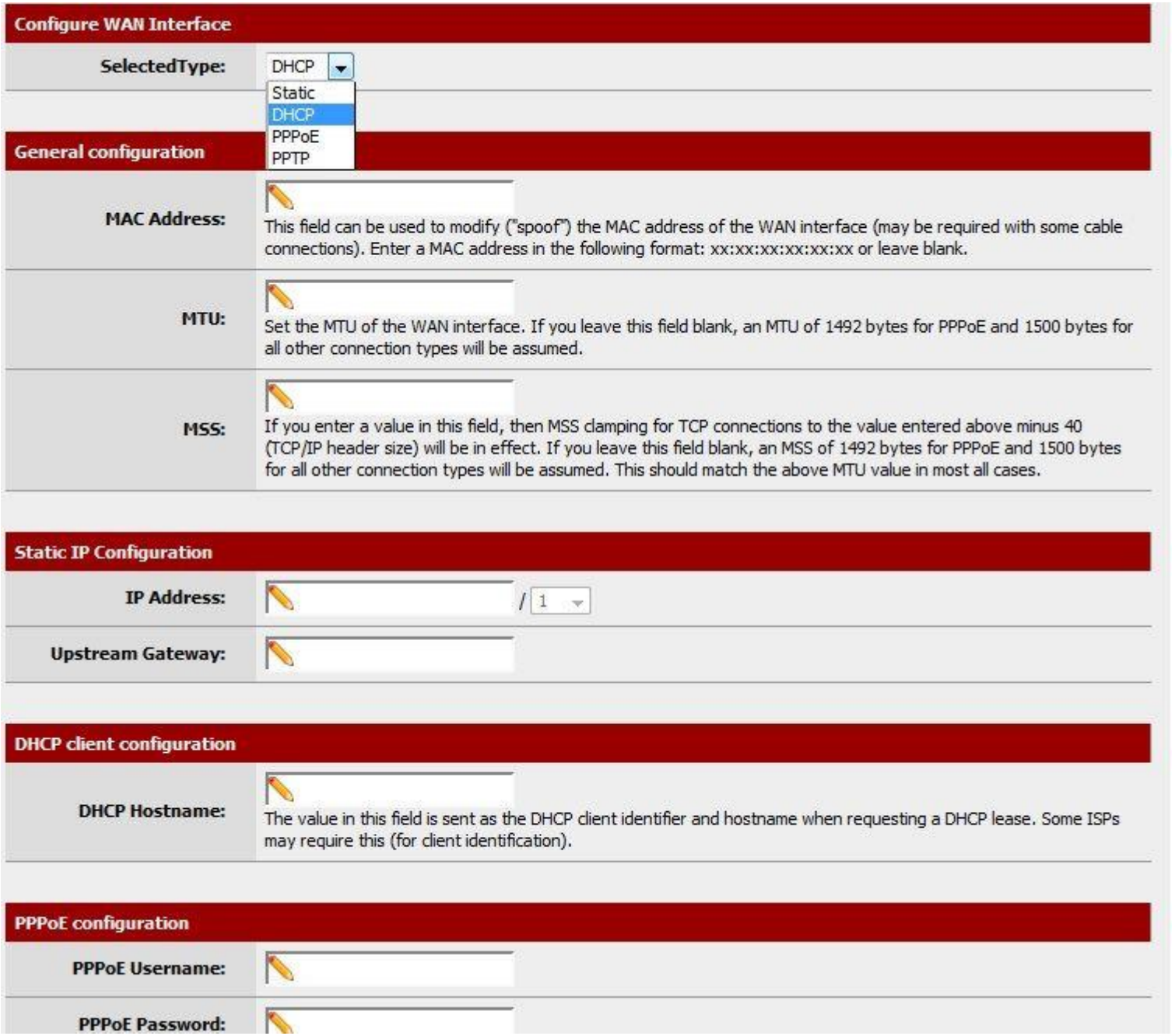
Nach erfolgtem Login ist man nun auf der KONFIGURATIONSOBERFLÄCHE.
Hier im *"General Setup"* kann man nun weitere Anpassungen am System (z.B. Passwörter etc.) vornehmen. Für einen ersten Test muss hier aber erstmal nichts mehr eingetragen werden !
Da pfSense auch selber ein vollständiger DSL-Router mit stateful Firewall Funktion ist, lassen sich im Menüpunkt WAN-INTERFACE auch direkt PPPoE Provider Zugangsdaten etc. eintragen um pfSense z.B. direkt an einem "nur" DSL-Modem zu betreiben !
Der direkte Anschluss an ein Kabel TV Modem eines TV Kabel Providers (WAN Port im DHCP Client Modus) ist damit ebenso leicht und problemlos möglich !
Auch hier ist für den ersten Funktionstest erstmal nichts einzutragen sofern ein LAN Router vor der pfSense betrieben wird !

Wer die Hotspot Firewall als solche in eine bestehende VLAN Struktur integrieren muss oder will, findet im folgenden eine detailierte Beschreibung wie das mit der pfSense genau zu machen ist:
https://www.administrator.de/wissen/vlan-installation-und-routing-mit-m0 ...

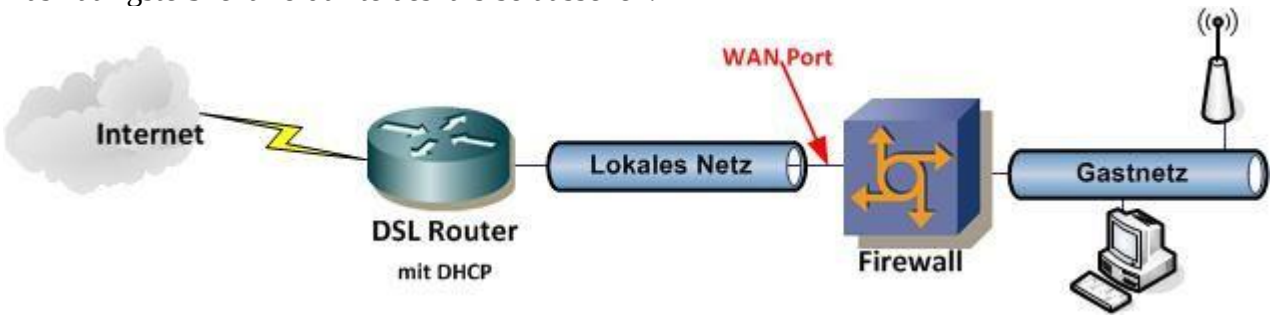
Noch ein Tip für die Installation auf einem ALIX Board !:
Die serielle Konsole die man auf diesem Mainboard am dort vorhandenen DB-9 Stecker hat bekommt man über ein serielles Terminalprogramm zu sehen. Wie das anzuschliessen und zu bedienen ist zeigt dieses Tutorial:
http://www.pfsense.org/mirror.php?section=/tutorials/wrap_install/wrap_ ...
oder https://www.administrator.de/contentid/149915 (Kapitel: *"Wenn nichts mehr geht"*)
(Achtung: Serielle Terminal Geschwindigkeit pfSense: 115.200 Baud !)

Installation in ein bestehendes Netzwerk mit Router

Ein häufiger Grund für Folgethreads hier im Forum ist die Integration dieses Captive Portals in bestehende IP Netze mit bestehendem DSL Router oder Modem und den fehlenden Einstellungen.
Deshalb hier ein paar zusätzliche Anmerkungen zu diesem wichtigen Thema:
Wie oben bereits angemerkt hat die Monowall und auch pfSense auf dem WAN/Internet Port mehrere Möglichkeiten der IP Adress Einstellung.


Configure WAN Interface
SelectedType:
DHCP
Static
DHCP
PPPoE
PPTP
General configuration
MAC Address:
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.
MTU:
Set the MTU of the WAN interface. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.
MSS:
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.
Static IP Configuration
IP Address:
/ 1
Upstream Gateway:
DHCP client configuration
DHCP Hostname:
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
PPPoE Username:
PPPoE Password:

Static = Statische IP Adressvergabe
DHCP = Automatische IP Adressvergabe durch vorgeschalteten Router
PPPoE = Direkt Kopplung mit einem reinen DSL Modem und Konfiguration der Provider Zugangsdaten direkt auf der Monowall
(PPTP = Spezielle Provider Zugangstechnik, wird in der Regel in D nicht verwendet)
Default ist die Einstellung auf DHCP, deshalb bekommt die FW bei der klassischen Kopplung an einen bestehen DSL Router von diesem auch eine IP mitsamt DNS.
Das häufigste Szenario dürfte deshalb so aussehen:



Hier gibt es ein paar grundsätzliche Dinge zu beachten:
1.)
Ist ein bestehender Router im Einsatz, benutzt dieser in der Regel immer private_IP_Adressen im LAN.
In dieses LAN Segment wird nun die Firewall gesteckt, die aber per Default an ihrem WAN Port einen Paket Filter auf genau diese privaten IP Adressen hat, da die Default Einstellung davon ausgeht das der WAN Port direkt am "gefährlichen" Internet ist und solche IP Adressen von dort nie kommen dürfen.
Ein Teil der wichtigen Sicherheitseinstellung der Firewall also !
Mit einer Routerkopplung davor ist das allerdings tödlich, denn es bewirkt das alle Daten vom lokalen LAN dann dort geblockt werden und nichts erreichbar ist. Ein häufiger Punkt für Nachfragen hier...
Wichtig ist also in solch einen Aufbau mit einem DSL Router davor (nicht bei einem reinen DSL Modem und direkter PPPoE Kopplung an den Provider !) diesen default Filter zu deaktivieren !

Das o.a. Bild zeigt in der WAN Interface Konfiguration wo dieser Haken des ***Private Adress Blocking*** zu entfernen ist !
Diese Punkte sollte man ebenso beachten:

2.)

Soll die FW als einfaches Captive Portal verwendet werden kann man die Einstellung des WAN Ports im DHCP Modus belassen und sich vom vorgeschalteten Router die IPs dynamisch vergeben lassen. Dafür ist einfach der WAN Port der FW mit dem LAN Port des Routers mit einem Patchkabel zu verbinden wie in Punkt 1. schon beschrieben.

3.)

Soll es **zusätzlich** einen VPN Zugang auf der Firewall für den remoten Zugriff von Clients auf das lokale Netzwerk geben oder einen Webzugriff für die Fernwartung mit der Monowall/pfSense eingerichtet werden, dann **muss** zwangsweise ein Port Forwarding (Port Weiterleitung) auf dem davorliegenden DSL Router gemacht werden um diese Port(s) an die FW weiterzuleiten.
Details zum Port Weiterleiten bei VPN findet man hier und hier oder auch hier im unteren Kapitel zur VPN Integration.
Hierbei macht es dann Sinn der FW dann immer statische IP Adressen auf dem WAN Port zu setzen, denn sollten sich die per DHCP empfangene WAN Adresse hier Aufgrund der Dynamik von DHCP einmal ändern, dann laufen die Port Weiterleitungen ggf. auf nichtexistente IP Adressen und damit ins Nirwana.
Aus diesem Grunde sind dann statische IP Adressen generell immer vorzuziehen wenn Port Weiterleitung im Spiel ist. Alternativ kann man natürlich über die Mac Adresse des WAN Ports auch immer feste IP Adressen im DHCP zuweisen sofern der Router davor sowas supportet. (DHCP

Mac Nailing)
Wichtig: Feste statische Adressen müssen **immer außerhalb** des DHCP Bereichs liegen, damit es nicht zu IP Adressüberschneidungen und Dopplungen kommt !

Ein weiterer, wichtiger Punkt der häufig zu Frust führt weil er vergessen wird:
Wird die WAN IP Adresse statisch konfiguriert, dann **MUSS** auch der DNS Server statisch konfiguriert werden !
Dies geschieht im Menü "General Setup":

System: General Setup

System

Hostname

pfSense

Name of the firewall host, without domain part
e.g. *firewall*

Domain

test.intern

Do not use 'local' as a domain name. It will cause local hosts running mDNS (avahi, bonjour, etc.) to be unable to resolve local hosts not running mDNS.
e.g. *mycorp.com, home, office, private, etc.*

DNS servers

DNS Server	Use gateway
	none
	none
	none
	none

Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS forwarder and for PPTP VPN clients.

In addition, optionally select the gateway for each DNS server. When using multiple WAN connections there should be at least one unique DNS server per gateway.

☑ **Allow DNS server list to be overridden by DHCP/PPP on WAN**
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). However, they will not be assigned to DHCP and PPTP VPN clients.

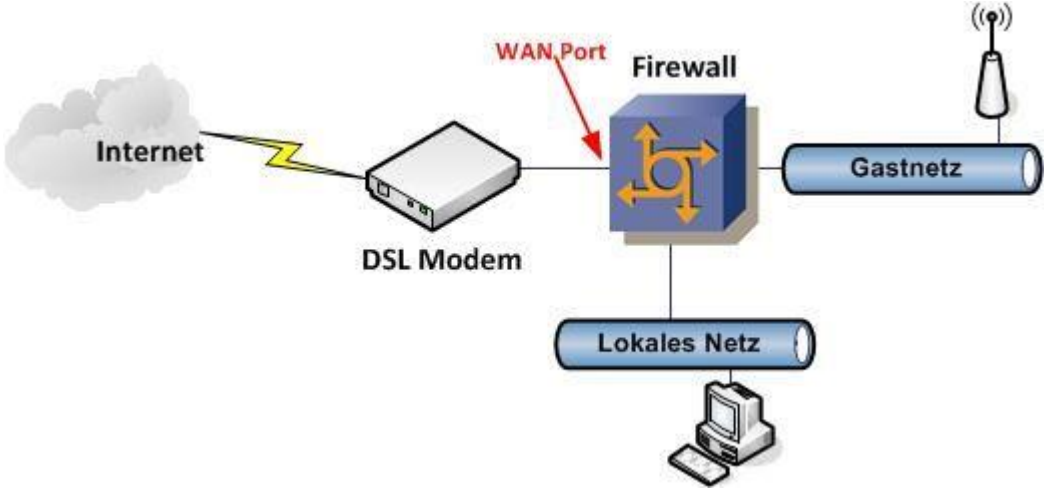
☐ **Do not use the DNS Forwarder as a DNS server for the firewall**
By default localhost (127.0.0.1) will be used as the first DNS server where the DNS Forwarder or DNS Resolver is enabled and set to listen on Localhost, so system can use the local DNS service to perform lookups. Checking this box omits localhost from the list of DNS servers.

Time zone

Europe/Berlin

Select the location closest to you

Wird vergessen den DNS einzutragen kommt es zu DNS Problemen und Fehlern bzw. Nichtfunktion beim Aufruf der Portalseite !
Wer komplett diese Probleme mit Port Forwarding umgehen will installiert die Firewall besser direkt am DSL Anschluss entweder mit einem einfachen, reinen DSL Modem oder indem er einen vorhandenen Router mit der PPPoE_Passthrough_Option in den Modem Modus konfiguriert.



Hier sind dann die PPPoE Zugangsdaten (Username / Passwort) **direkt** auf der Firewall im WAN Port Setup zu konfigurieren.
Damit entfallen dann alle zusätzlichen Port Weiterleitungsmassnahmen, da jetzt natürlich kein NAT Router mehr vor der FW ist und diese direkt am Internet hängt.
Los gehts mit dem Hotspot Gastnetz Setup...!

Captive Portal Setup

Wichtiger Test vorweg: Bevor man jetzt das Captive Portal (Hotspot Funktion) aktiviert sollte das o.a. Firewall Szenario sauber funktionieren !
Ein Client im LAN Segment angeschlossen sollte dazu mit seiner von der pfSense vergebene IP problemlos ins Internet gelangen können.
Erst wenn DAS sauber funktioniert sollte das CP aktiviert werden um ggf. zusätzliche Netzwerk Fehler vorher sicher ausschliessen zu können und Frust und überflüssige Fehlersuche zu vermeiden !!

Nächster Anlaufpunkt ist die Seite zur Einrichtung und Aktivierung des CAPTIVE-PORTALS also der Hotspot Funktion.

Man erstellt zuerst mit Klick auf "+" ein Captive Portal Profil, wo man das Interface festlegt auf dem das CP wirken soll und geht dann in die eigentliche CP Konfiguration.

Folgende Einträge müssen zwingend dabei gemacht werden:

- Haken bei *"Enable Captive Portal"* setzen um die Captive Portal Funktion zu aktivieren !
- Idle Timeout oder Hard Timeout auf den gewünschten Wert setzen. (Idle Timeout ist die Zeit der Inaktivität eines Benutzers ab wann das Portal den Zugang für eingeloggte Benutzer wieder sperrt, Hard Timeout ist ein fester Zeitwert nachdem der Benutzer vom Gastzugang zwangsweise getrennt wird und sich neu einloggen muss.)
- *Authentication* sollte im ersten Schritt immer auf *Local User Manager* gesetzt sein. Im Local User Manager oder oben im Karteireiter *"Users"* kann man dann dort seine lokalen CP Benutzer anlegen oder für Hotels, Cafes, etc. eine VoucherID (Einmalpasswort) aktivieren. Später ist hier dann auch eine sehr komfortable Benutzerverwaltung und Accounting mit einem Radius Server möglich wie z.B. dem Microsoft NPS (ex IAS) oder Freeradius !

Hinweise zur Installations eines FreeRadius Servers gibt ein entsprechendes Security_Tutorial hier bei Administrator.de.

- Bei **Portal Page Contents**. Kann man die Portalseite entsprechend anpassen um dort nur User/Passwort oder nur Voucher oder beide Optionen abzufragen.

Sinnvoll bei Gästen ist eine NUR Voucher Funktion mit Einmalpasswörtern die einem eine aufwendige User und Passwort Verwaltung erspart. Im HTML Code ist das dann entsprechend auszukommentieren oder zu löschen.
Entweder lebt man hier also mit dem Default, besser ist aber immer eine kleine, eigene HTML Datei zu importiertieren, die eine eigenes Logo, Bilder oder Informationen enthält, also auf seine Gastbesucher angepasst ist. Man sollte nicht vergessen das so eine Portalseite immer die "Visitenkarte" ist und einen ersten Eindruck vermittelt !

Der folgende HTML Code ist eine einfache HTML Login und VoucherID Abfrage (HTML Datei), die man einfach mit Klick auf ***Quelltext*** (-> Oben rechts im Balken des Textblocks !) und dann cut and paste oder direkt mit *in Speicher kopieren* mit einem Editor in eine reine Textdatei sichert und diese dann z.B. login.html nennt.
Je nach Anforderung kann hier der Title Text und andere Texte im Editor den persönlichen Erfordernissen und Einsatzzweck angepasst werden.
(Achtung: unbedingt darauf achten das die Datei wirklich **login.html** heisst und nicht z.B. login.html.txt o.ä. !)
HTML Unkundige brauchen hier also keinerlei Angst zu haben und nur markieren und kopieren....
Mit einem einfachen Notepad Editor kann man die Texte in dieser Datei auf die eigenen Bedürfnisse umgestalten

Dann wird diese HTML Datei gesichert und mit dem Button **Choose File/Datei auswählen** im CP Setup im Menüpunkt **"Portal Page Content"** (Captive Portal Seite) über das Webinterface per Mausklick auf die Firewall hochgeladen.
Nun nur noch unten unbedingt den **Save** Button klicken um alles zu sichern !!
Sucht man bei Google nach *"captive portal examples"* findet man weitere grafisch ansprechnde Beispiele.
Wer will spart sich das, muss dann aber mit der relativ schlichten Default Seite leben.

Hier die zu kopierende HTML Beispiel Datei zur Portal Seite:

Quelltext | Drucken


```
01. <HTML>
02. <HEAD>
03.         <TITLE>Administrator.de (Gast WLAN Zugang)</TITLE>
04. <style>
05. b, i {
06.         font-family: Helvetica;
07. }
08. i {
09.         font-size: 8pt;
10. }
11. </style>
12. </HEAD>
```

```
13.
<BODY leftMargin=0 topMargin=0 marginwidth="0" marginheight="0">
14.
<TABLE height=15 cellSpacing=0 cellPadding=0 width=660 border=0>
15.
<TR>
16.
        <TD vAlign=top width=1 bgColor=#7F00B2>
17.
        </TD>
18.
</TR>
19.
</TABLE>
20.
<TABLE cellSpacing=0 cellPadding=0 width=700 border=0>
21.
<TR>
22.
        <TD vAlign=top width=303><IMG src="logo.jpg" border=0></TD>
23.
        <TD vAlign=center height="21" width="700">
24.

25.
        <b style="font-size: 16pt"> WLAN Internet Gast Zugang</b><br>
26.
        <b style="font-size: 12pt">Bitte geben sie Benutzernamen und Passwort an</b><br>
27.
        <b style="font-size: 10pt">Beachten Sie das WLAN Verkehr über dieses Portal NICHT verschlüsselt ist !</b>
28.
        </font>
29.
        </TD>
30.
</TR>
```

```
</TABLE>
<TABLE height=15 cellSpacing=0 cellPadding=0 width=660 border=0>
<TR>
        <TD vAlign=top width=1 bgColor=#7F00B2>
        </TD>
</TR>
</TABLE>
<TR>
<TD vAlign=top width=200>
</TD>
<TD vAlign=top width=20></TD>
<TD vAlign=top width=398><br>
<form method="post" action="$PORTAL_ACTION$">
<TD class=largetext vAlign=center width = 70>
                <b>User ID:</b>
<input name="auth_user" type="text">
</TD>
<TD class=largetext vAlign=center width =70>
```

```
                <b>Password:</b>
<input name="auth_pass" type="password">
</TD>

<TD class=largetext vAlign=center width =70>
                <b>Voucher ID:</b>
<input name="auth_voucher" type="text">
</TD>

<br><br><br>
<input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
<input name="accept" type="submit" value="Continue">
</form>
                <TR>
                <TD class=copytext vAlign=center colSpan=10>
                <i>Copyright &copy; 2015, Administrator.de</i>.</TD>
                </TR>
</TD>
```

```
67.
<TD vAlign=top width=10></TD>
68.
</TR>
69.
<TABLE height=15 cellSpacing=0 cellPadding=0 width=660 border=0>
70.
<TR>
71.
<TD vAlign=top width=1 bgColor=#3300B2>
72.
</TD>
73.
</TR>
74.
</TABLE>
75.
</BODY>
76.
</HTML>
```

Will man z.B. die Username / Passwort Abfrage komplett unterdrücken weil man NUR Voucher Zugang will kommentiert man diesen Part aus dem HTML Code aus (Zeile 48) oder löscht schlicht und einfach diese Zeilen !


```
<!-- //// Für nur Voucher so auskommentieren ///
<TD class=largetext vAlign=center width =70>
                <b>Password:</b>
<input name="auth_pass" type="password">
</TD>
-->
```

Der in der o.a. HTML Datei befindliche Logobild Dateiname (hier das abgeb. *WiFi* Logo) *"logo.jpg"* muss man ggf. mit einem individuellem Dateinamen seines eigenen verwendeten Firmen- oder persönlichen Logos ersetzen wie z.B. *"firmenlogo.gif"* oder *"firmenlogo.jpg"* wenn die Logo Datei so heissen sollte.
HTML Anfänger können aber auch hier wieder ihre Logo Bilddatei vom Dateinamen ganz einfach umbenenen in *logo.jpg* und ersparen sich so an der o.a. HTML Datei die Änderungen und können sie einfach übernehmen !

Über den Karteireiter "File-Manager" lädt man diese oder weitere Logo Dateien, die in der Portalseite verwendet werden sollen, auf die Firewall.

Vorsicht !!
Auch hier lauert der Teufel im Detail ! Vor dem Hochladen heisst eine Datei *logo.jpg* die dann nach dem Upload ***captiveportal-****logo.jpg* von der FW umbenannt wird !
Das muss man im HTML Text unbedingt beachten, denn sonst sieht man nachher statt des Bildes einen leeren Platzhalter im Browser !
Ein Rechtsklick auf den Platzhalter und "Informationen" enthüllt dann wie das Logo eigentlich heisst.
Der Logo Dateiname muss also im HTML Text immer korrekt eingegeben werden. Groß- Kleinschreibung ist hier relevant !

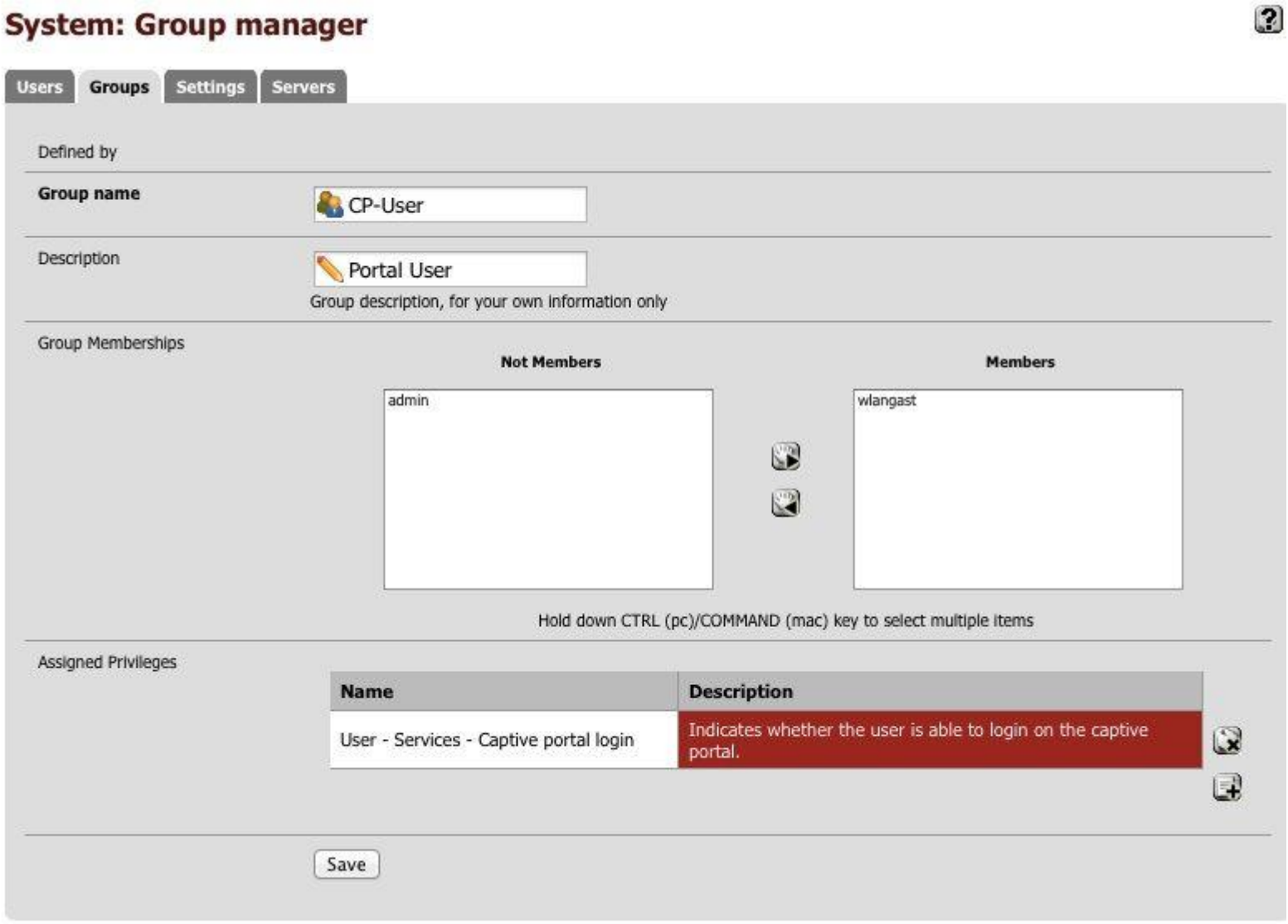
Diese Hotspot Login Seite kann jeder entsprechend nach individuellen Anforderungen HTML-technisch ausschmücken, so das Hotels, Cafes oder Firmen dort noch spezifische Informationen z.B. rechtlicher- oder anderer Art plazieren können.
Hotels / Campingplätze / Cafes etc. können so Benutzer auf Angebote, Aktivitäten usw. aufmerksam machen. Auch das Nachladen von externem Content, von remoten Webservern wie Grafiken oder wechselnde Texte ist problemlos möglich.
Ebenso eine Zwangs Weiterleitung nach dem Hotspot Login auf externer oder interne Firmen, Hotel, Cafe Webserver ist per Mausklick möglich um Kunden auf spezifischere Infos aufmerksam zu machen die evtl. dort gehostet und upgedatet werden.
HTML Webprogrammierern und HTML *Spezies* sind hier keinerlei Grenzen in der Gestaltung gesetzt !
Hilfe für HTML Anfänger bietet hier z.B. eine Seite wie Self-HTML
Unten in den weiterführenden Links befindet sich eine Anleitung zum automatischen Versenden der Vouchers per SMS auf Mobiltelefone der Anwender. Auch solch einen Link kann man in der Portalseite plazieren.

Wichtig ist nun unten unbedingt wiederum den **SAVE** Button zu klicken um diese Einstellungen zu sichern !
Spezifische Bilder wie z.B. die o.a. Logos und Bilddateien sind oben über die *"File Manager"* Funktion einfach upzuloaden. Wichtig ist das die Dateinamen mit denen im HTML File absolut übereinstimmen damit die Grafik angezeigt wird ! (Groß- Kleinschrift !)

Der Hotspot Betrieb:

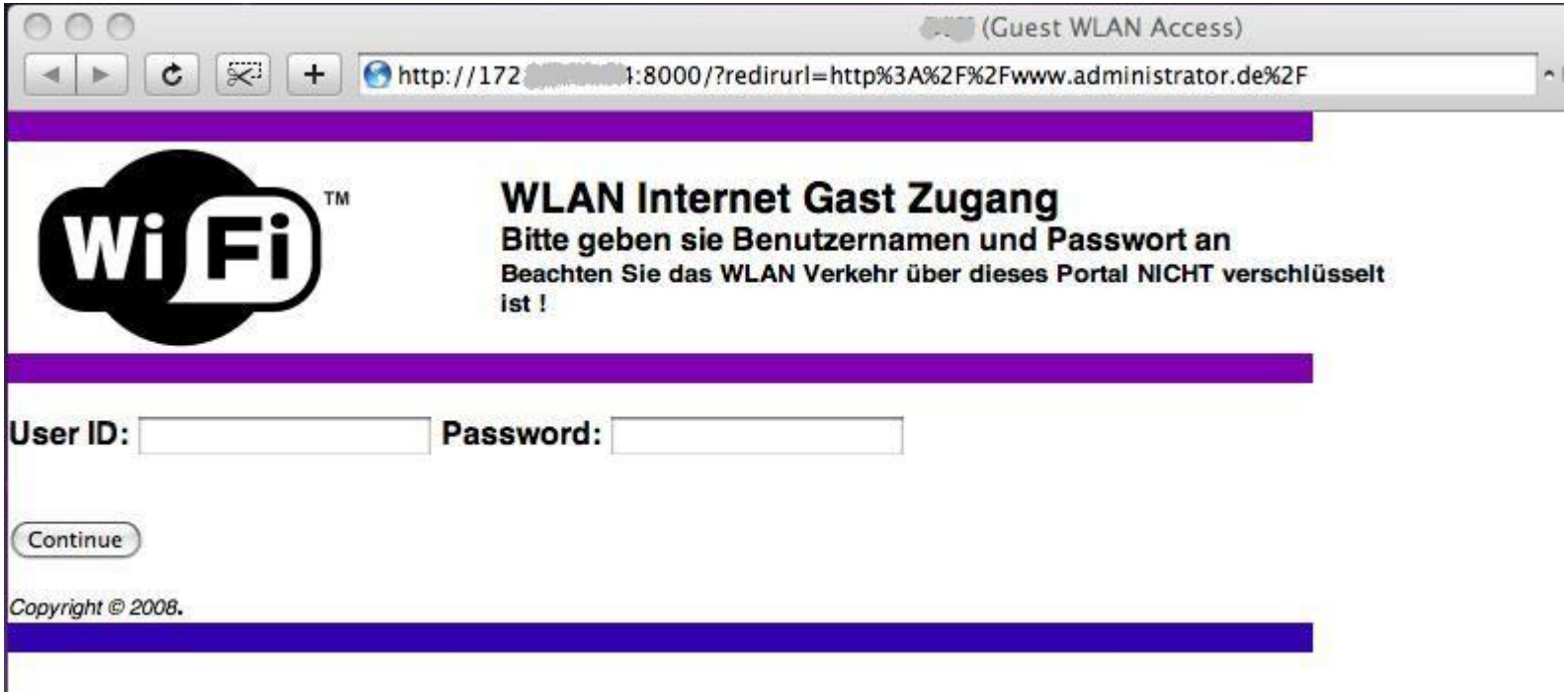
Sind nun Benutzer bzw. Voucher Zugang eingerichtet und das Captive Portal mit HTML Login Datei aktiviert, steht einem ersten Test nichts mehr im Wege !
Achtung: Ab der Version 2.1 der pfSense sind die Portaluser die man in der Userverwaltung einrichtet mit einem Attribut *"User - Services - Captive*

portal login" zu versehen ! Am besten legt man dort eine extra Gruppe an für die Portaluser und definiert sie dort:



Vorher sollte man noch unbedingt den Browsercache löschen, damit Seiten nicht lokal aus dem Cache aufgerufen werden können !

Wenn man jetzt z.B. mit dem Browser auf www.administrator.de geht erscheint **nicht** Administrator.de sondern zuerst die Hotspot Login Seite des Captive Portals, die so aussieht wie in der Abb. unten. Verwendet man die o.a. HTML Datei mit Logo (Hier im Beispiel das WiFi Symbol als *logo.jpg* Datei !):



(Die o.a. Seite bezieht sich vom Inhalt auf einen WLAN Zugang, gilt aber natürlich analog auch für einen Zugang über ein Kupfer/Kabel Segment (LAN).
Erst wenn man hier sauber mit Benutzernamen und Passwort (wie im User Manager gesetzt) authentifiziert ist, gelangt man automatisch weiter zu Administrator.de...oder eben anderen Webseiten.
Funktioniert alles, ist das Captive Portal damit einsatzbereit !

Bequeme Verwaltung: Einmal Passwörter (Voucher) für Gäste verwenden !

Eine sehr interessante und überaus nützliche Funktion des Portals ist die Verwendung von sog. *Vouchers* (Einmalpasswörtern) für Gastbenutzer !
Hotels, Campingplätze, Cafes oder Firmen die externe Gäste oder Benutzer haben, können so eine sog. einmalige Voucher ID vergeben, die einem Gast den einmaligen und zeitlich limitierten Zugang erlaubt. Danach verfällt das Passwort automatisch.
Nach Ablauf dieser Zeit wird der Zugang getrennt. So ist sichergestellt das Username und Passwort einzelner Benutzer nicht mißbräuchlich weitergegeben werden können und man hat ein Usertracking (Störerhaftung in D) um rechtlich abgesichert zu sein.
Es können mehrer Voucher Zeiten auf einmal installiert werden so das man Voucher mit 30 Min., 1 Std. usw. vergeben kann.
https://doc.pfsense.org/index.php/Captive_Portal_Vouchers
Nach der Generierung kann die Voucher Datei als Excel CSV Datei mit Klick auf das kleine **blaue "i"** im Voucher Setup exportiert werden.
Die komfortabelste und auch sinnvollste Lösung zur Verwaltung und Ausgabe dieser Voucher mit einer Web basierten Lösung bequem per Browser, beschreibt ein separates Tutorial hier im Forum:
https://www.administrator.de/contentid/193763
Das beinhaltet sogar den automatischen Versand dieser Voucher ID auf ein Mobiltelefon per SMS.
So ist die Ausgabe dieser Einmal Passwörter auch für ungeübtes Personal kinderleicht.

Eine weitere Voucher Erstellung über ein externes Excel Sheet was man gut ausdrucken kann z.B. für den Verkauf etc., findet man hier im Download:
http://ts-telecom.net/voucherdrucker.xls
(Dank an Forumsmitglied ThorstenTS der es freundlicherweise zur Verfügung gestellt hat ! Siehe auch unten im Thread Verlauf)
Eine andere Möglichkeit ist die bequeme Voucheradministration und Druck mit einer MS Office Access Anwendung die Formumsmitglied SarekHL hier dem Forum dankenswerter Weise ebenfalls zum Download zur Verfügung gestellt hat.
Auch einen Möglichkeit des direkten Ausdrucks über die pfSense Webseite findet sich in den weiiterführenden Links unten.
(Bei Fragen zu diesen Tools bitte per Personal Mail direkt an die Verfasser wenden !)

Welcher Gast, wann und wie lange eingeloggt war, kann man bequem über die Benutzer Statusseite nachverfolgen:

Oder über das komfortable Dashboard der pfSense:

Status: Dashboard

System Information

Name	pfsense[redacted]ntern
Version	**2.1.2-RELEASE** (i386) built on Thu Apr 10 05:23:54 EDT 2014 FreeBSD 8.3-RELEASE-p15 You are on the latest version.
Platform	nanobsd (2g)
NanoBSD Boot Slice	pfsense1 / ad0s2 (rw)
CPU Type	Geode(TM) Integrated Processor by AMD PCS
Uptime	22 Hours 48 Minutes 20 Seconds
Current date/time	Sun Apr 13 15:38:33 CEST 2014
DNS server(s)	127.0.0.1 [redacted]
Last config change	Sat Apr 12 16:50:05 CEST 2014
State table size	0% (3/10000) Show states
MBUF Usage	9% (390/4416)
Load average	0.24, 0.07, 0.02
CPU usage	3%
Memory usage	51% of 107 MB
Disk usage	21% of 907M

Interfaces

WAN	100baseTX <full-duplex> [redacted]
CPLAN	100baseTX <full-duplex> 10.10[redacted]

Captive Portal Status

IP address	MAC address	Username

Interface Statistics

	WAN	CPLAN
Packets In	3247	0
Packets Out	3687	0
Bytes In	299 KB	0 bytes
Bytes Out	2.35 MB	0 bytes
Errors In	0	0
Errors Out	0	0
Collisions	0	0

Auch der aktuelle Interface Traffic und andere Betriebsdaten lassen sich ebenfalls über das einstellbare Dashboard beobachten.
Mit der Firewall ist ein TRAFFIC-SHAPING möglich, um Gast Benutzern nur eine bestimmte Bandbreite zuzuteilen um andere Nutzer und Anwendungen z.B. aus dem Firmennetz nicht zu beeinträchtigen !

Da das FW Setup auch aus dem Gastnetz zugänglich ist, empfiehlt es sich natürlich zwingend im Livebetrieb das Administratoren Passwort zu ändern und im GENERAL-SETUP ggf. auch den Setup Zugang mit einer HTTPS Verbindung und ggf. einem anderen Port wie dem Standardport bei HTTPS wie z.B. TCP 54443 abzusichern.
Am sichersten ist es den GUI Zugang zur Firewall aus dem Gastnetz ganz zu verbieten und nur vom Verwaltungsnetz an einem anderen Port zuzulassen !

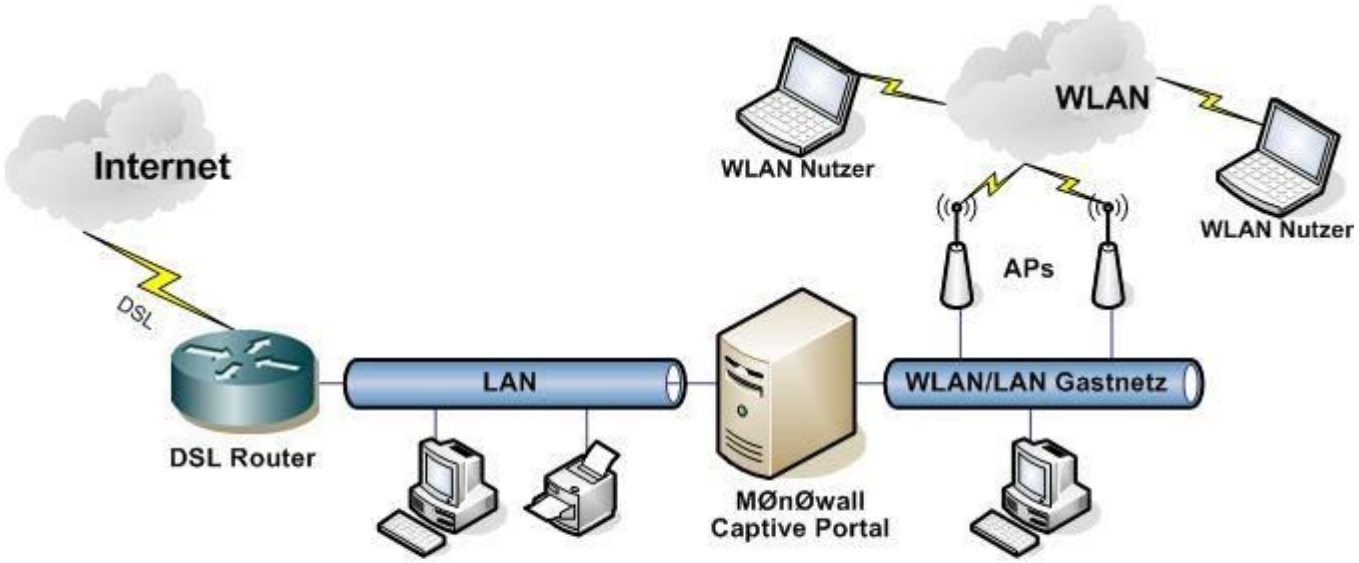
- Zu diesem Punkt der lokalen Administrator Zugriffsteuerung hat unser Forumuser "tikayevent" richtigerweise noch folgende bessere Variante vorgeschlagen:

Du verlagerst das Webinterface auf einen anderen Port. Es gibt aber eine andere und bessere Möglichkeit:
Wenn man im Advanced Menü die "Antilockout-Regel" abschaltet, kann man den Zugang per Firewall für das Gast-Netz blocken.
Bei sämtlichen Captive Portal-Installationen, die ich mit m0n0wall bisher gemacht habe, habe ich wie folgt gearbeitet:

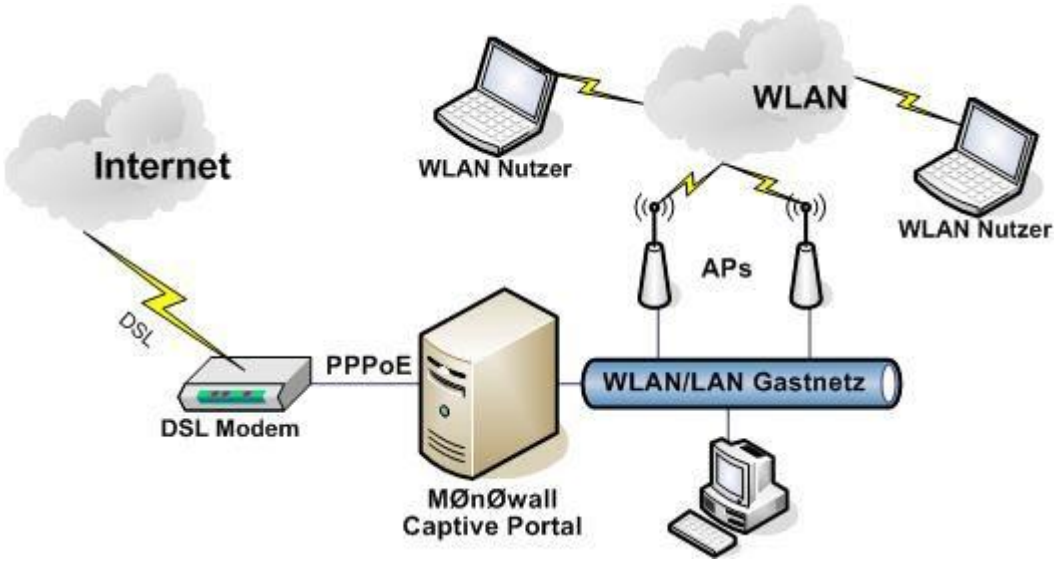
- Antilockout-Rule deaktiviert
- sämtlichen Traffic auf den Router geblockt
- TCP/UDP 53 auf den Router erlaubt
- TCP 8000 (Captive-Portal-Port) auf den Router erlaubt

Damit kommt man nicht an das Webinterface dran, egal wie sehr man sucht und es funktioniert trotzdem alles.

Wer keine sichere DMZ Variante benötigt, kann auch ein etwas einfacheres Szenario aufbauen wie dieses hier:



Da, wie bereits oben bemerkt, pfSense ein kompletter DSL- oder auch Kabel Router mit PPPoE und PPTP Support ist, bietet sich auch ein Design ganz ohne extra DSL Router an, indem man den M0n0wall Rechner direkt an ein vorhandenes DSL- oder Kabel TV Modem anschliesst. Ein solches Netz zeigt die folgende Abbildung:



(Ein separates zusätzliches DMZ Segment ist ebenfalls mit einer dritten Netzwerkkarte oder VLAN_Support möglich !)

Firewall Regeln (Filter) richtig setzen !

Aufgrund vieler Threads zu diesem Thema folgt an dieser Stelle ein kleiner Exkurs zum richtigen Setzen der Firewall Regeln.
Für das Einstellen der Firewall Filter (Rules) auf den Interfaces gibt es immer 2 wichtige Grundbedingungen zu beachten:

- **1. Die Regeln wirken nur auf eingehende Pakete IN die Firewall !** Also nur auf Pakete die IN das Interface hineingehen (Incoming)
- 2. Das Regelwerk arbeitet nach dem sog. **"First Match Wins"** Verfahren ! (Der erste Treffer gewinnt)

Letzteres bedeutet das sobald eine Regel positiv ist (matched), die weiter folgenden Regeln **NICHT** mehr abgearbeitet werden.
Folglich ist damit die **Reihenfolge** der Regeln am Port nicht mehr trivial, also beliebig, sondern essentiell wichtig für die korrekte Funktion der Firewall Regeln am bereffenden Port !
Man kann also NICHT in der ersten Regel alles erlauben (denn das wäre ein "Match") und dann in weiteren Regeln Einschränkungen machen,

sondern muss es genau andersrum machen:
Zuerst die Einschränkungen und dann erlauben.
Nicht vergessen: Ist KEINE Regel an einem Port definiert, blockt die Firewall im Default **ALLES** wie es für eine gute Firewall üblich ist !
Das folgende Beispiel (Screenshot pfSense) ist die klassische Anforderung und macht die Funktion klar:
Es wird ein Gastnetz betrieben (hier im Beispiel der Port VLAN-10) und am LAN Port ein privates Netzwerk auf das die Gäste keinerlei Zugriff haben dürfen:

Floating | LAN | WAN | VLAN10

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		*	VLAN10 net	*	LAN net	*	*	none		Zugriff aufs private Netz verbieten
		TCP/UDP	VLAN10 net	*	*	53 (DNS)	*	none		DNS erlauben
		TCP	VLAN10 net	*	*	80 (HTTP)	*	none		HTTP erlauben
		TCP	VLAN10 net	*	*	8000	*	none		Portalseite erlauben
		TCP	VLAN10 net	*	*	443 (HTTPS)	*	none		HTTPS erlauben

Das "x" an der ersten Regel zeigt das es eine BLOCK Regel ist. Pakete vom VLAN-10 IP Netzwerk, also dem Gastnetzwerk, mit dem Ziel privates Netzwerk (LAN Port) werden geblockt.
Desweiteren dürfen aus diesem Gastnetz nur Pakete zur Namensauflösung (DNS, UDP/TCP 53), zum Surfen (HTTP, TCP 80), zum sicheren Surfen (HTTPS, TCP 443) und die Portalseite (TCP 8000, ACHTUNG: **8002** ab Release 2.2 !!) des Hotspots passieren.
Ein recht restriktives Gastnetz also, in dem nur Surfen erlaubt ist. Alles andere wird geblockt.

Gastlogins zum Nachweis mitprotokollieren

Eine weitere zentrale Frage vieler Folgethreads ist die Lösung der Protokollierung der Gastlogins. Da die Störerhaftung rechtlich noch nicht abgeschafft ist, ist das immer eine Überlegung wert die jeder vor dem öffentlichen Betrieb eines Hotspots über einen Privatanschluss anstellen sollte.
Diese hier vorgestellte Firewall hat aber die bequeme Möglichkeit per Syslog alle diese Meldungen über einen sehr langen Zeitraum nachweissicher auf einen Logging Server im Netzwerk zu schreiben.
Viele preiswerte Heim NAS Systeme (QNAP, Synology usw.) die oft schon im privaten Netz als Medienserver usw. vorhanden sind, haben einen Syslog Server an Bord der nur per Mausklick im Setup aktiviert werden muss und so diese Meldungen aufzeichnet. Sie stellen die einfachste aber nicht immer preiswerteste Lösung dar.
Eine andere sehr kostengünstige und effiziente Methode zur Lösung wird mit diesem_Logging_Server_Tutorial hier im Forum beschrieben. Dieser Server arbeitet sehr sparsam im Netz im Nonstop Betrieb und hat keine beweglichen Teile. USB Ports für einen optionalen zusätzlichen Speicherstick sind gleich mit an Bord und bei Bedarf kann er noch weitere Aufgaben im Netz übernehmen.
Natürlich funktionieren auch andere Lösungen mit freier Syslog Server SW wie KiwiSyslog, Draytek Syslog, TFTP32 und dem Mikrotik Syslog, die man kostenfrei aus dem Internet laden kann.

Optional: Erweiterung des Captive Portals mit einem integrierten WLAN Accesspoint :

Vorbemerkung zur WLAN Erweiterung:
Die Installation eines WLAN Moduls in das ALIX Board ist KEIN Muss um das Captive Portal im WLAN zu betreiben !!
Man kann genauso gut WLAN Accesspoints oder zum Accesspoint_gemachte_WLAN-Router direkt an die M0n0wall anschliessen (LAN oder OPT Port) um ein und dasselbe zu erreichen !
Bei größeren Hotspot Lösungen mit mehreren WLAN Accesspoints ist dann klar die technisch bessere Lösung !
Nun weiter mit der Integrationsanleitung....

Bei Verwendenung des o.a. ALIX Minimainboards (oder auch eines PCs mit WLAN PCI Karte) ist es möglich der M0n0wall Appliance gleich ein WLAN Accesspoint mit *einzupflanzen*. Man erhält so eine handliche "Allround Appliance" als *eierlegende Wollmilchsau* die universell einsetzbar ist.
Sie kann z.B. in kleinen Cafes, Restaurants usw. als integrierte *"all in one"* DSL Router mit gleichzeitiger Hotspot Funktion dienen, die lediglich für den Betrieb noch ein billiges passives DSL Modem am Provider Anschluss erfordert.

(Man sollte unbedingt beachten das bei größeren WLAN Installationen mit mehreren Accesspoints dies weniger Sinn macht, da die APs dann in einem eigenen Netz abgesetzt vom CP an der Monowall betrieben werden sollten.)

Diese *WLAN Aufrüstung* ist problemlos und sehr einfach möglich, da das o.a. ALIX 2Cx Minimainboard bereits einen entsprechenden miniPCI Sockel besitzt für die Aufnahme eine WLAN miniPCI Karte.
Ferner hat das o.a. Gehäuse gleich passend eine Bohrung für den WLAN Antennenanschluss so das keinerlei mechanische Arbeiten anfallen !
So liegt es nahe in kleineren Hotspot Installationen die Appliance gleich WLAN fähig zu machen und sich einen externen Accesspoint zu sparen, wenn man keine größere WLAN Infrastruktur (Ganze Hotels, Firmen oder Campingplätze etc.) mit dem Captive Portal absichern möchte.
Letzteres erfordert dann ja so oder so, wie bereits angemerkt, meistens mehrere externe WLAN Access Points.
Der Einbau ist auch von Laien sehr einfach zu bewerkstelligen.

Bei Verwendung von Standard PC Hardware für diese Firewall wird einfach statt einer miniPCI Karte eine ganz normale PC WLAN PCI Karte von der Stange in den PC eingebaut. M0n0wall oder pfSense erkennt diese beim Booten automatisch !
Damit eine korrekte Funktion sichergestellt ist, sollte die WLAN PCI Steckkarte am besten mit **Atheros, Intel, PRISM, oder Ralink Chipsatz** ausgerüstet sein !!

Kompatible WLAN PCI Karte Karten findet man z.B. HIER
Die im Firewall_Tutorial genannten Bezugsquellen bieten allesamt preiswerte zertifizierte WLAN miniPCI Steckkarten für das ALIX Board an.
http://varia-store.com/Hardware/MiniPCI-Karten:::637_67.html
Hier kann man beim Kauf also definitiv nichts falsch machen !

Los gehts mit dem Zusammenbau...

Die Einbauschritte beim ALIX Mini Mainboard sind einfach zu erledigen:

1.) Ein passendes miniPCI WLAN Modul mit Atheros beschaffen wie z.B. dieses hier:

Diverse_Auswahl
oder
Wistron_DCMA81
(Dieses Modul bedient sowohl den 5 Ghz als auch den 2,4 Ghz WLAN Bereich !)

2.) Dazu passend wird ein Antennen Pigtail (Kabel mit U.FL Stecker auf R-SMA Buchse) benötigt:

https://shop.tronico.net/WirelessLAN/Pigtails/ oder http://shop.varia-store.com/index.php?cat=c174_RP-SMA--SMA--Clip.html
oder
http://varia-store.com/Zubehoer/Pigtails-Verbindungskabel:::638_68.html

und eine passende WLAN Aufsteckantenne:
https://shop.tronico.net/WirelessLAN/Antennen/ und http://shop.varia-store.com/index.php?cat=c85_Rundstrahl--Dipol.html

Oder jegliche andere WLAN Andenne intern oder auch extern die auf die verwendete Pigtail R-SMA Buchse passt !!
Eine Auswahl leistungsfähiger Antennen findet man z.B. hier:
http://www.wimo.de/uebersicht-wlan-antennen_d.html
Wer beide WLAN Bänder (2,4Ghz b/g und 5Ghz a) gleichzeitig bedienen will, nimmt eine Dual Band Aufsteckantenne wie diese:
http://www.wimo.de/wlan-dualband-antennen_d.html (Equipment antenna Dualband 2.4/5GHz)
die dann gleichzeitig das 2,4 Ghz und auch das 5Ghz Band bedient !
Wenn weitere Entferneungen überbrückt werden müssen oder für den Außenbereich dann eine externe Antenne.

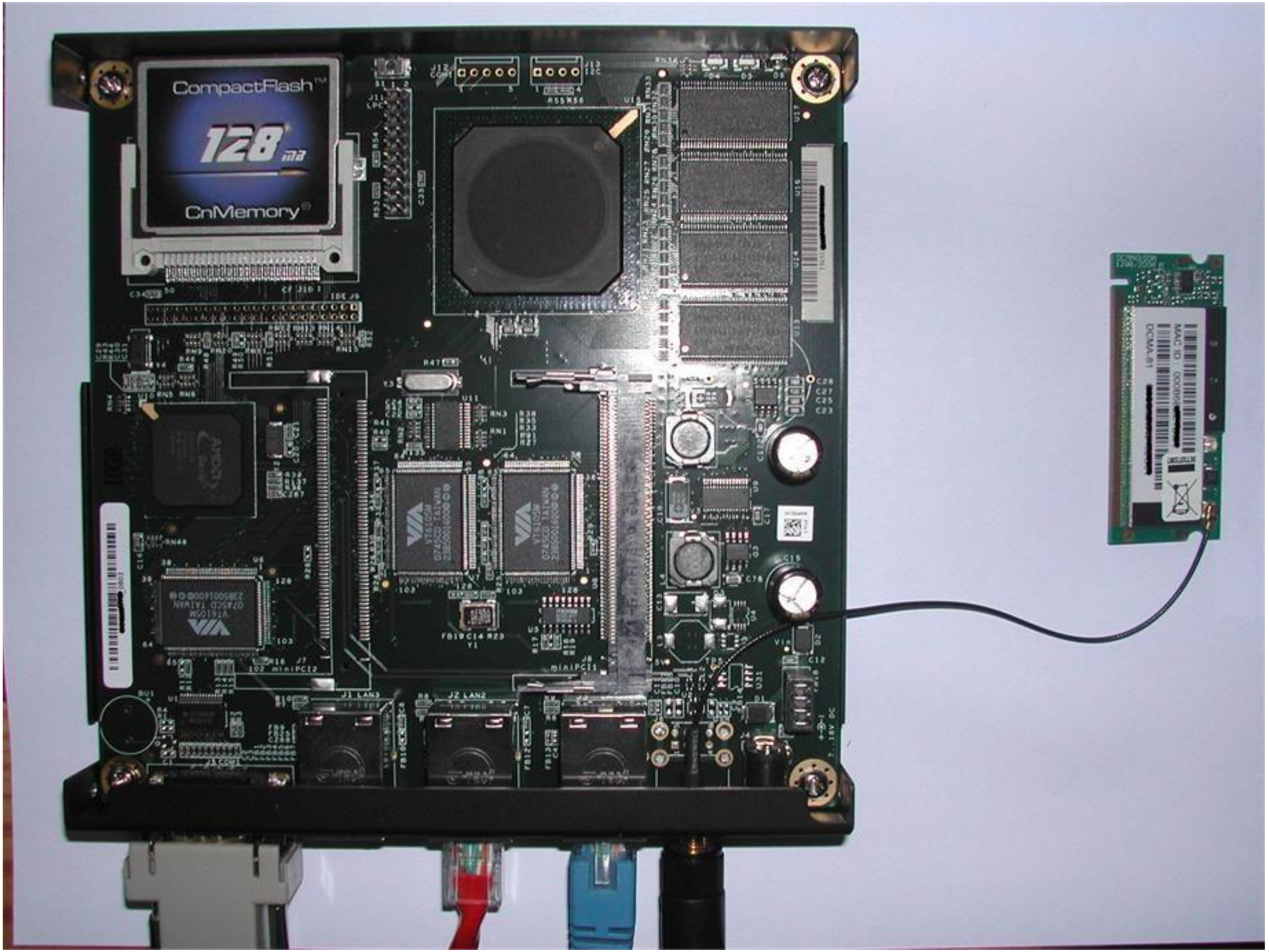
Alle Teile zusammensetzen

3.) Die Endmontage:

Das Pigtail (Kabel mit beiden Antennensteckern) schraubt man nun in die dafür vorgesehene Bohrung im Gehäuse und schliesst den kleinen U.FL Antennenstecker durch einfaches Aufdrücken an das miniPCI Modul an.
Die o.a. miniPCI WLAN Module haben 2 Antennenbuchsen (Diversity)
Das Wistron mit der Bezeichnung **J2** (äußere Buchse) und **J3** (innere Buchse).
Der U.FL Stecker des Pigtail Antennenkabels wird auf die **innere Buchse** (die am Abschirmkäfig, links !) gesteckt.
(**Achtung: Hier im Bild ist der Antennenanschluss fälschlicherweise an der rechten Buchse angeschlossen muss aber auf die linke !!!)**

Beim TP Link Modul ist es einfacher dort haben die Buchsen die Bezeichnung ***MAIN*** und ***AUX*** und der Anschluss erfolgt immer an die Buchse ***MAIN*** !
Im Zweifelsfall muss man beide Buchsen ausprobieren, sollte man ein anderes Modul verwenden.

Am einfachsten misst man dann die Feldstärke in einiger Entfernung mit dem WLAN Sniffer WLANINFO oder noch besser mit dem iSSIDer der eine bessere grafische Anzeige besitzt und prüft mit welcher Antennenbuchse die Funk Feldstärke und Reichweite am höchsten ist !
Der Unterschied ist meist drastisch und sofort sichtbar in der Anzeige !


CompactFlash
128 MB
CnMemory

(Abbildung zeigt das ALIX Mainboard mit separatem WLAN miniPCI Modul)

Ist alles verbunden wird das miniPCI Modul in den entsprechenden Sockel auf dem ALIX Board gesteckt:


CompactFlash
128 MB
CnMemory
MAC ID
DCMA-81

(Abbildung zeigt das ALIX Mainboard mit fertig montiertem WLAN miniPCI Modul und Antenne)

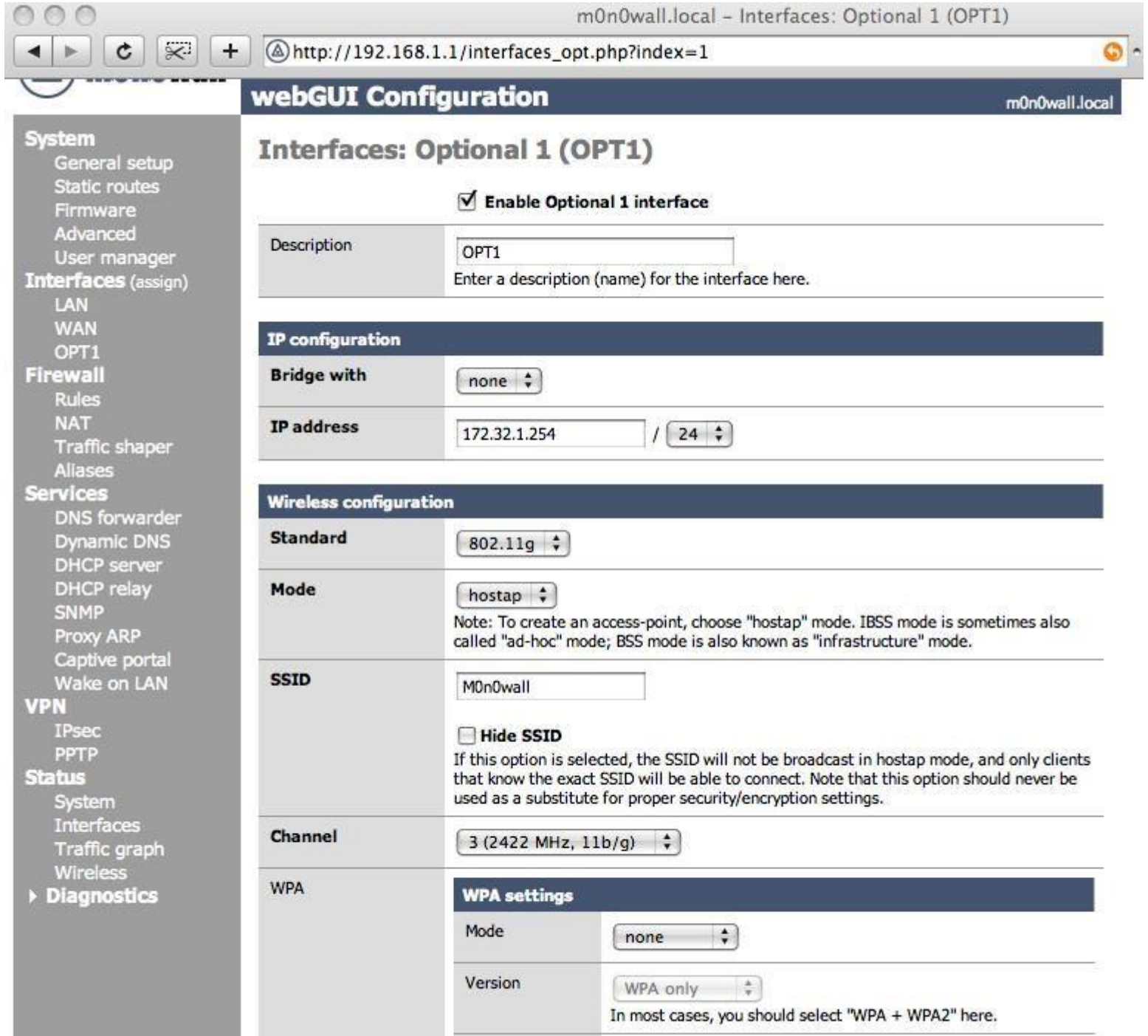
Fertig machen zum WLAN Funken !

4.) WLAN im Setup aktivieren

Jetzt ist nur noch das Web Interface aufzurufen im Browser und hinter **Interfaces** im Menü auf *"assign*" zu klicken. Danach klickt man im Menü rechts auf das + Zeichen und fügt so das Interface hinzu.

Die Monowall erkennt das Interface beim Starten automatisch selber. Im Menü taucht dann im Fenster "Network Port" sowas wie *ath0 (Atheros 5212, 00:0b:6b:2e:1c:67* auf das die erkannte Karte und dessen Mac Adresse auflistet.

das OPT1 Interface nun im Interface Setup aktivieren und ihm eine IP Adresse zuweisen. In der "Description" kann man den Namen OPT1 gegen das sinnvollere *WLAN* ersetzen, damit gleich klar ist im Setup um welches Interface es geht !


m0n0wall.local - Interfaces: Optional 1 (OPT1)
http://192.168.1.1/interfaces_opt.php?index=1
webGUI Configuration
m0n0wall.local
System
General setup
Static routes
Firmware
Advanced
User manager
Interfaces (assign)
LAN
WAN
OPT1
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
Interfaces: Optional 1 (OPT1)
Enable Optional 1 interface
Description
OPT1
Enter a description (name) for the interface here.
IP configuration
Bridge with
none
IP address
172.32.1.254
/
24
Wireless configuration
Standard
802.11g
Mode
hostap
Note: To create an access-point, choose "hostap" mode. IBSS mode is sometimes also called "ad-hoc" mode; BSS mode is also known as "infrastructure" mode.
SSID
M0n0wall
Hide SSID
If this option is selected, the SSID will not be broadcast in hostap mode, and only clients that know the exact SSID will be able to connect. Note that this option should never be used as a substitute for proper security/encryption settings.
Channel
3 (2422 MHz, 11b/g)
WPA
WPA settings
Mode
none
Version
WPA only
In most cases, you should select "WPA + WPA2" here.

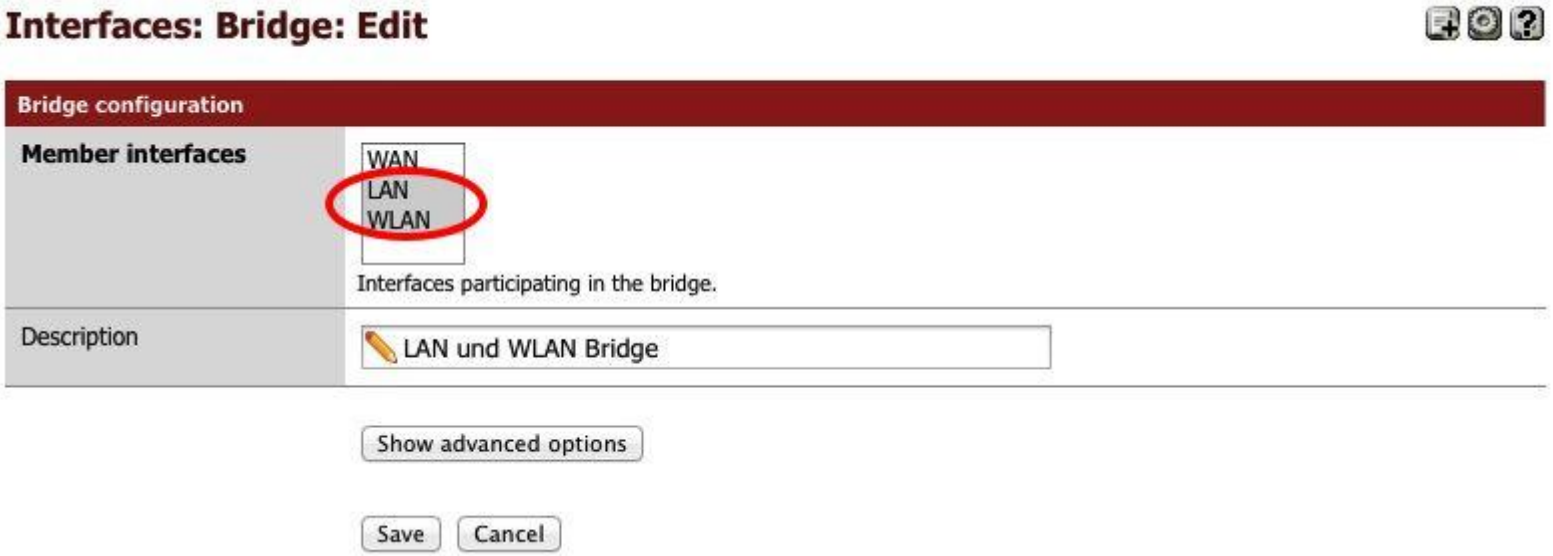
Damit werden dann sofort die WLAN Settings aktiv.
Hier kann man nun nach Wahl die SSID (WLAN Kennung), Verschlüsselung usw. einstellen.
Achtung: Im DHCP Setting nicht vergessen DHCP für dieses Interface (OPT1) zu aktivieren damit IPs im WLAN automatisch von der M0n0wall vergeben werden !
Mit einem WLAN-Scanner(WLANINFO) oder iSSIDer kann man nun sein WLAN *in der Luft* sehen ebenso wie im WLAN Auswahlmenü und sich mit dem WLAN verbinden.
Zu beachten ist dann nur unbedingt einen Abstand von 5 Kanälen zu evtl. vorhandenen Nachbar WLANs zu halten um Störungen zu vermeiden !
Das o.a. inSSIDer Tool zeigt die Verteilung der Funkkanäle !
Die Schritte bei der Installation auf Standard PC Hardware sind identisch !

LAN und WLAN im gleichen IP Netz betreiben mit einer Bridge:

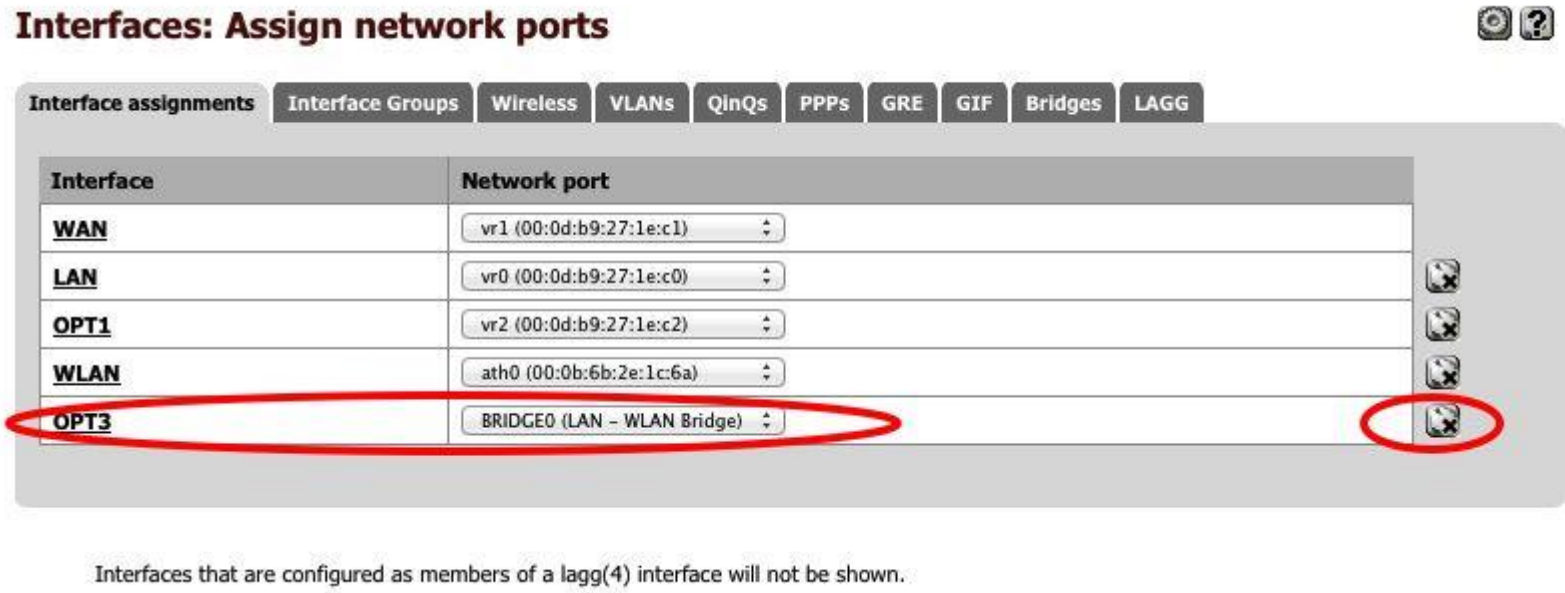
Normal ist das WLAN ein eigenständiges Interface mit eigenem IP Netzwerk. Oft ist es aber wünschenswert wie bei den gängigen WLAN Routern den LAN und WLAN Port in einem gemeinsamen Netz zu betreiben. Das erreicht man mit einem Bridge Interface (Netzwerkbrücke).
Hier müssen die IP Adresse und die FW Regeln vom LAN Interface auf ein einzurichtendes Bridge Interface gelegt werden das LAN und WLAN Port mit einer sog. "Netzwerkbrücke" transparent verbindet ! Netzwerker nennen sowas eine "Layer 2 Bridge".
Dazu sollte man die folgenden Schritte möglichst genau der Reihe nach befolgen:

- 1.) WLAN Interface wie oben beschrieben einrichten und aktivieren im "Access Point" Mode, Regulatory Domain ETSI, Country "Germany/ETSI" (ändern bei anderen Ländern !) und .11g Mode only (oder .11n) sowie SSID anlegen. **Achtung:** IPv4 Adressing bleibt hier auf **none** !

- 2.) Nun ein Bridge Interface anlegen unter "Interface assign" mit Klick auf "Bridge". Hier wählt man den LAN und fügt **mit gedrückter Shift Taste** den WLAN Port hinzu. Beide Ports der Bridge werden blau unterlegt. Man ergänzt einen Namen und klickt "Save" zum Sichern:



- 3.) Jetzt fügt man das Bridge Interface wieder unter dem Menüpunkt "Interface assign" den Interfaces global hinzu mit Klick auf "+" rechts und klickt wieder "Save" zum Sichern:



- 4.) Man wählt mit Klick auf das Bridge Interface dies aus und aktiviert es (Haken), gibt ihm einen eindeutigen Namen z.B. *"WLAN Bridge"* , stellt das IPv4 Adressing auf ***Static*** und vergibt der Bridge eine neue IP Adresse im gleichen 192.168.1er Netz z.B. **192.168.1.254** mit 24 Bit Maske und klickt "Save" (ggf. die IP Adresse an die eigenen Belange anpassen !)

Interfaces: WLANBridge

General configuration

Enable	**Enable Interface**
Description	WLANBridge Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC address	Insert my local MAC address This field can be used to modify ("spoof") the MAC address of this 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
MTU	If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

Static IPv4 configuration

IPv4 address	192.168.1.254 / 24
IPv4 Upstream Gateway	None - or **add a new one.** If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the link above. On local LANs the upstream gateway should be "none".

- 5.) **! Achtung !:** Um sich jetzt nicht selbst den (IP) Ast abzusägen auf dem man sitzt **MUSS** man jetzt unbedingt die Firewall Regeln für das Bridge Interface definieren, denn FW üblich ist hier alles **verboten** !

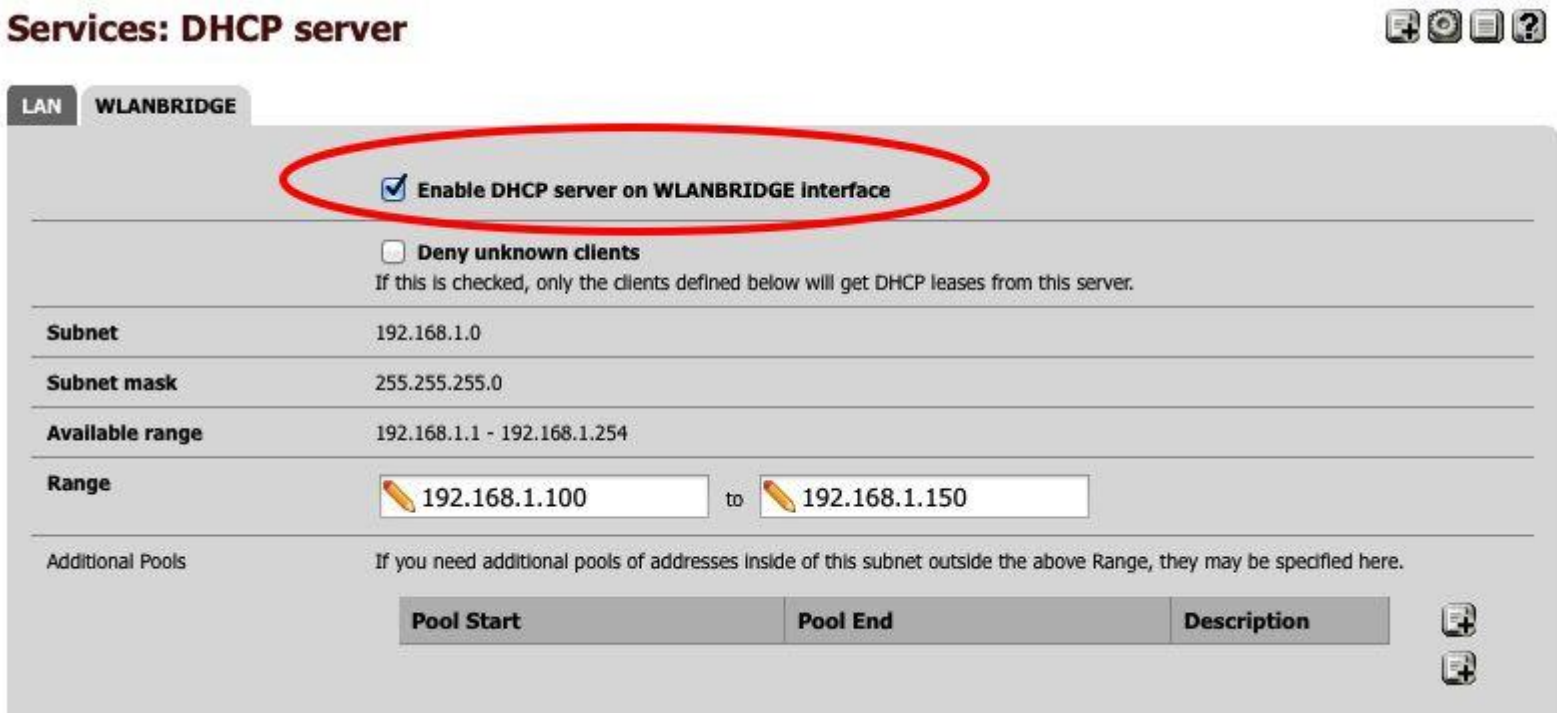
Hier im Beispiel ist jetzt analog zu den LAN Port Default Rules alles aus dem Bridge Netz erlaubt. Diese FW Regel muss man dann ggf. später anpassen will man hier Einschränkungen für den Zugang machen !:

Firewall: Rules: Edit

Edit Firewall rule	
Action	Pass 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.
Disabled	**Disable this rule** Set this option to disable this rule without removing it from the list.
Interface	WLANBRIDGE Choose on which interface packets must come in to match this rule.
TCP/IP Version	IPv4 **Select the Internet Protocol version this rule applies to**
Protocol	any Choose which IP protocol this rule should match. Hint: in most cases, you should specify *TCP* here.
Source	**not** Use this option to invert the sense of the match. Type: WLANBRIDGE net Address: /
Destination	**not** Use this option to invert the sense of the match. Type: any Address: /
Log	**Log packets that are handled by this rule** Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).
Description	WLAN-LAN Bridge Traffic erlauben You may enter a description here for your reference.

Save Cancel

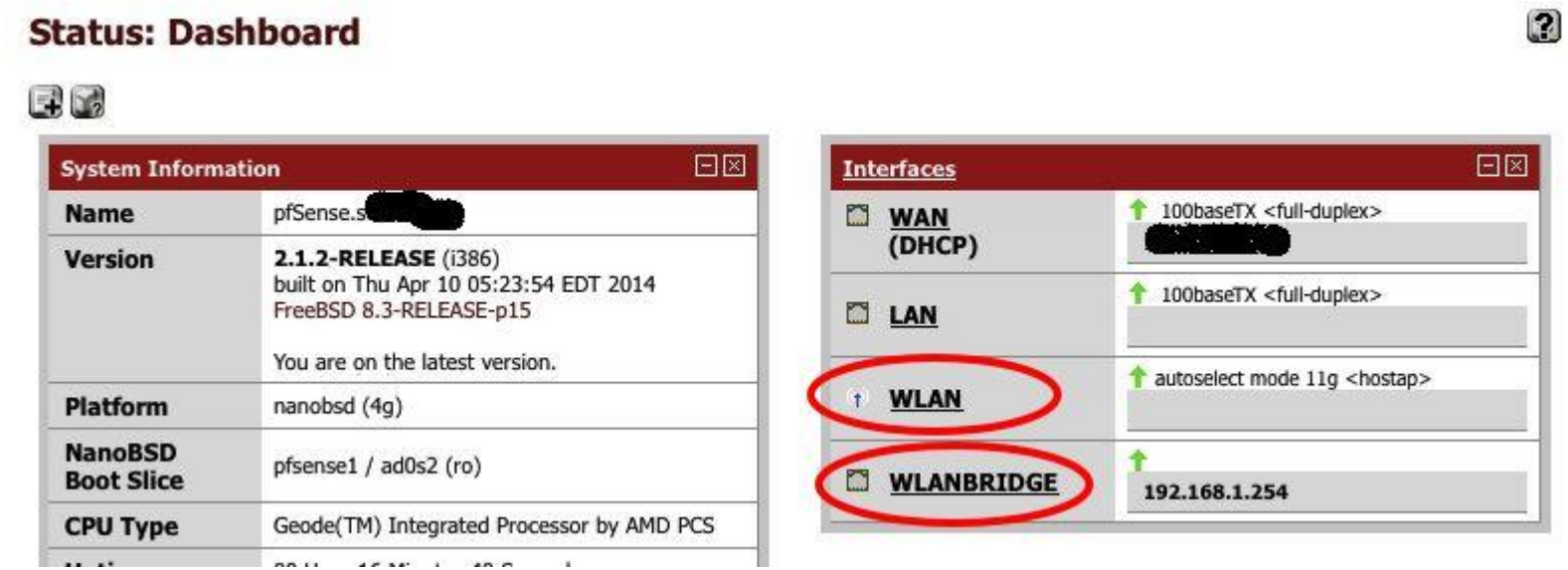
- 6.) Da der DHCP Server noch auf dem LAN Interface verknüpft ist muss dieser dort unbedingt **deaktiviert** werden (Haken entfernen) und auf dem Bridge Interface wieder aktiviert werden:



- 7.) Damit ist dann das IP Readressing vom LAN auf das Bridge Interface (LAN-WLAN Verbindung) abgeschlossen und man kann nun auch auf dem LAN Interface die .1er IP Adresse deaktivieren, was mit einem beherzten Klick auf **none** im Adress Setting dieses Interfaces geschieht !

Auch hier Achtung, denn wenn man auf "Apply Settings" geht ist die pfSense erstmal "weg" im Browser, da es die .1er IP ja nun nicht mehr gibt aber keinen Angst...
Man eröffnet einfach eine neue Browser Session auf die Bridge IP **192.168.1.254** und hat sie pfSense dann wieder hat man oben alles richtig gemacht

- 8.) Fertig...das wars ! Sieht man sich jetzt das Dashboard an sieht man auch das aktive Bridge Interface:



Erschliesst sich einem nicht sofort wenn man es das erste Mal macht, denn es ist nicht sofort klar das die IP Adressen nun am Bridge Interface aufgehängt werden statt an einem der physischen Ports !
WLAN und LAN arbeiten nun im gleichen IP Segment wie man es von fast allen gängigen WLAN Routern kennt.
Will man ein Gast LAN über dieses Interface sowohl kabelbasiert als auch WLAN basiert betreiben muss das CP natürlich auch am Bridge Interface aktiviert werden.

Dual Band AP Betrieb bei einer WLAN miniPCI Karte die 2,4 Ghz und 5 Ghz WLAN supportet:

Der sog. Dual Radio Betrieb, also das der interne WLAN AP parallel sowohl im 2,4 Ghz als auch im 5 Ghz WLAN Bereich arbeitet, wird ähnlich wie oben auch über eine Bridge gelöst die beide WLAN Radios einer Mini PCI Karte zusammenfassen in ein gemeinsames WLAN Netz.
Aktuelle mini PCI Module sind heute oft sog. "Dual Radio" Module, die sowohl das 2,4 Ghz als auch das 5 Ghz WLAN Band parallel abdecken.
Bei Verwendung eines solchen Modules muss man das 5 Ghz Band mit einem **Wireless "Parent Interface"** aktivieren mit den folgenden Schritten

(Beispiel mit pfSense OS !):
1.)
Nachdem man grundsätzlich das WLAN Modul bzw. Interface mit einem Klick auf "+" unter *Interface -> assign* aktiviert hat, muss man dieses fest auf 802.11**g** Betrieb setzen, Type auf "none", Mode auf "Accesspoint" Regulatory Domain "ETSI" und Country auf "Germany/ETSI" ! Danach aktiviert man das Interface mit Klick auf *enable Interface*.
Man kann den Interface Namen dann ggf. von *"OPT2"* auf *"WLAN-2.4Ghz"* ändern um die Bezeichnung eindeutiger zu machen.
Achtung: Ab der aktuellen 2.1.2 Firmware hat sich das Menü etwas geändert und die Wireless Parent Interfaces richtet man unter dem Karteireiter "Wireless" im Menüpunkt "Interface assign" ein. Die Installations Schritte sind aber identisch.
2.)
Jetzt klickt man wie bereits gesagt unter "Interface -> assign" auf den Reiter "Wireless" und dann auf "+" und fügt das Parent Interface für das 5 Ghz Band hinzu was man z.B. "WLAN-5Ghz" nennt.
3.)
Danach klickt man unter Interfaces -> assign wieder auf "+" und fügt dieses Parent Interface global zur Liste hinzu und aktiviert es mit Klick auf *enable*
4.)
In den WLAN Settings setzt man dieses Interface aber diesmal fest auf **802.11a** (a = 5Ghz WLAN), der Rest, Type auf "none", Mode auf "Accesspoint" Regulatory Domain "ETSI" und Country auf "Germany/ETSI" bleibt identisch zu den Settings auf 2,4 Ghz.
ACHTUNG: Den 5 Ghz Funkkanal sollte man entweder auf Auto lassen oder immer die UNTERN 8 Kanäle unter Kanal 100 im 5 Ghz Bereich wählen wie z.B. den **Kanal 48** wenn man feste Kanäle vergibt wie bei APs in der Regel üblich !
Grund ist das viele WLAN Karten und Module im 5_Ghz_Band nicht das ganze Band abdecken sondern immer nur die unteren 8 Kanäle. Hier also aufpassen !
Mit freien WLAN Scannern wie dem inSSIDer oder WiFi_InfoView kann man immer die korrekte Sendefunktion in beiden Bändern kontrollieren !
Apple Mac hat einen eingebauten_Scanner ebenso wie Linux.
5.)
Nun wechselt man in die Bridge Konfiguration unter *Interfaces assign* und fügt man die 2 WLAN (oder 3 wenn man z.B. mit einem LAN Interface bridgen möchte) Interfaces zusammen *WLAN-2,4*, *WLAN-5* und, wenn erforderlich, das entsprechende LAN Interface (3tes Interfaces) ! (Auswahl mit gedrückter Shift Taste)
Beide WLAN Interfaces und ggf. bei Bedarf ein LAN Segment, fügt man mit der Bridgefunktion zusammen wenn man sie gemeinsam in einem IP Netz nutzen will:
6.)
Auf Interfaces assign -> Bridges klicken und mit "+" eine Bridge bzw, Bridge Interface hinzufügen.
7.)

Interfaces auswählen die zusammen gebridged werden sollen. Hier die beiden WLAN Interfaces. Wer es mit einem LAN Interface bridgen will wählt dieses optional dazu (Shift Taste gedrückt halten und Klick)
8.)
Bezeichnung der Bridge eintippen z.B. "Bridge WLAN-LAN".
9.)
Unter Interfaces auf "assign" klicken und das neue Bridge Interface mit Klick auf "+" wieder global hinzufügen.
10.)
Jetzt auf Interfaces, das Bridge Interface auswählen und den Haken bei "Enable Interface" aktivieren ! Ggf. die Bezeichnung auf etwas sinnvolles wie "WLANBridge" statt OPTx ändern)

Mit einem WLAN Scan Tool wie dem bereits genannten *inSSIDer* oder *WiFiInfoView* kann man nun beide WLAN Signale senden sehen !
Wichtig hier falls es Probleme gibt die *Kanal 48* Regel oben für 5 Ghz zu beachten.
Die Linksammlung unten verweist auf einen Forums Thread mit Screenshots dazu.

Zusatzfunktionen: VPN Zugang und LAN-LAN Kopplung per VPN, VLAN Integration

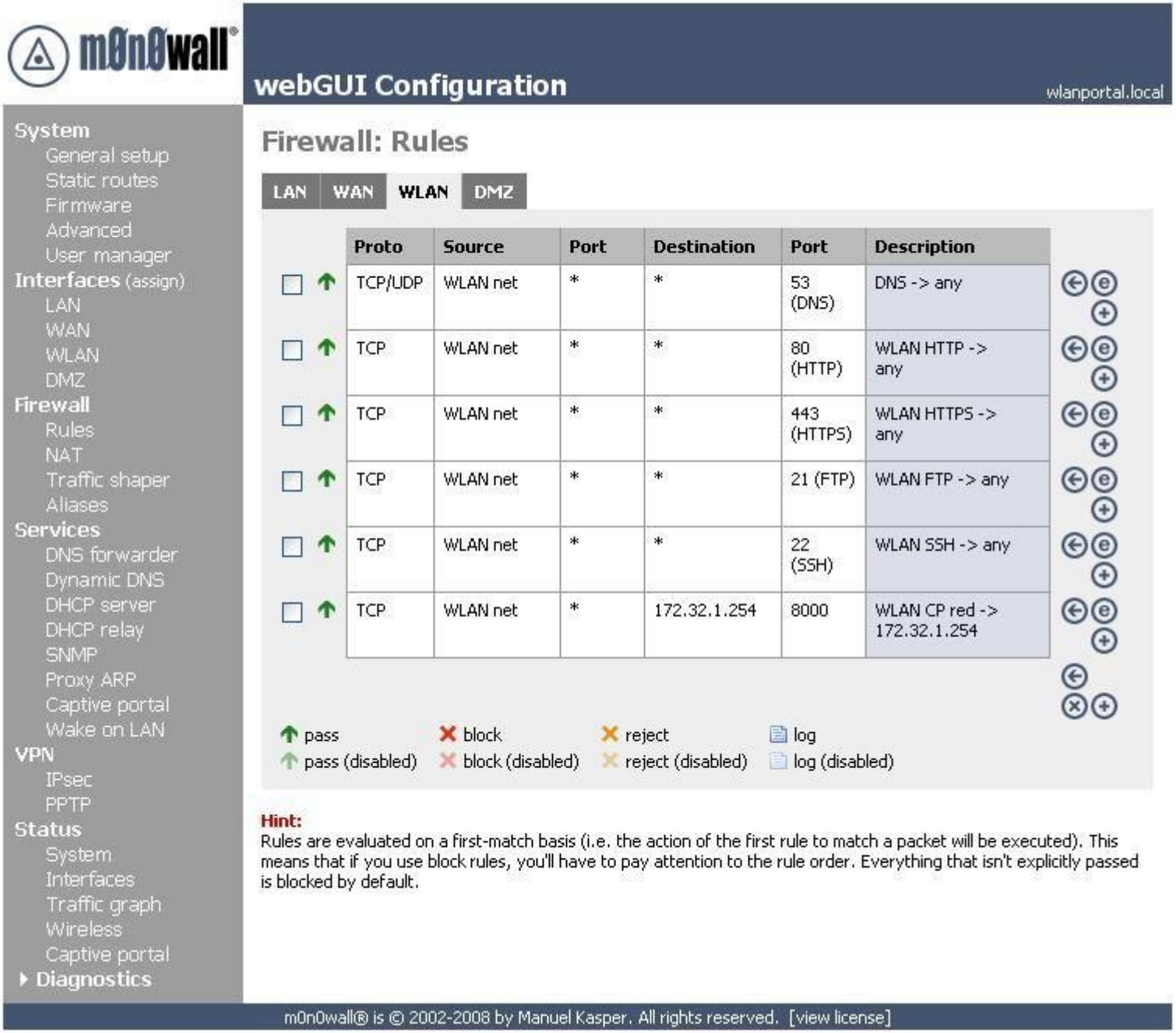
Als zusätzlichen *Bonbon* bietet die Monowall und auch die pfSense Firewall einen VPN Zugang zur VPN Kopplung mit anderen Monowalls, pfSense und allen IPsec fähigen Firewalls oder VPN Routern am Markt wie z.B. (Cisco, Fritzbox, Draytek etc.) zur Firmen Standortvernetzung mit einer LAN zu LAN Kopplung.
Oder natürlich auch die Kopplung von VPN Clients für den Netzzugriff von remoten, mobilen Benutzern mit Laptops oder Smartphones oder zur sicheren Fernwartung eines Netzes..
Wie dies zusätzlich zu realisieren ist erklären hier im Forum 2 separate Tutorials im Bereich Firewall und Sicherheit...

Für den PPTP VPN Zugang oder allgemein VPNs mit PPTP Protokoll. PPTP und IPsec Clients haben alle aktuellen Betriebssysteme und Smartphones heute von sich aus an Bord.
Eine Installation zusätzlicher VPN Clientsoftware ist bei PPTP somit nicht erforderlich ! Eine VPN Installation bzw. Funktion ist so im Handumdrehen auf der Firewall und Client quasi mit *Bordmitteln* installiert.

Wer etwas gehobenere Ansprüche an die Sicherheit stellt, verwendet das IPsec Protokoll für den VPN Zugang:
Für den VPN Zugang mit IPsec
Als IPsec VPN Client bietet sich alternativ zur einfacheren PPTP Variante der kostenlose Shrew IPsec VPN Client an. IPsec gilt gemeinhin als sicherer im Vergleich zu PPTP. Wie damit ein einfacher Zugriff auf die M0n0wall realisiert wird ist hier zu sehen:
http://www.shrew.net/support/wiki/HowtoMonowall
pfSense bietet zudem noch die Option eines OpenVPN Servers und Clients. Wie ein OpenVPN Server mit pfSense installiert und aktiviert wird erklärt wie ein separates Forumstutorial im Detail:
https://www.administrator.de/index.php?content=123285

Last but not lease beschreibt das VLAN Tutorial die Integration in eine bestehende VLAN Umgebung:
https://www.administrator.de/contentid/110259

ACHTUNG: Wichtig um Frustrationen gleich zu vermeiden: !!
Wie bei einer Firewall allgemein üblich, sind zusätzliche Interfaces (Ausnahme nur das LAN Interface !) wie die zusätzlichen OPTx Interfaces per Default IMMER vollkommen **geblockt**. Kein IP Verkehr kommt also von diesen Interfaces durch die Firewall ohne das man die Firewall Regeln zu diesem Interface anpasst !!
Damit man nun nach der erfolgreichen Einrichtung des WLAN (oder auch eines DMZ/OPT Interfaces) keinen Riesenfrust erleidet weil nichts funktioniert muss **VORHER** immer eine Firewall Regel eingerichtet werden !
Für unser WLAN Interface wird also folgende Firewall Regel in den Firewall Rules für das WLAN Interface aktiviert um einige Standardfunktionen zu erlauben !!!:


m0n0wall
webGUI Configuration
wlanportal.local
System
General setup
Static routes
Firmware
Advanced
User manager
Interfaces (assign)
LAN
WAN
WLAN
DMZ
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
LAN
WAN
WLAN
DMZ
Proto
Source
Port
Destination
Port
Description
TCP/UDP
WLAN net
*
*
53 (DNS)
DNS -> any
TCP
WLAN net
*
*
80 (HTTP)
WLAN HTTP -> any
TCP
WLAN net
*
*
443 (HTTPS)
WLAN HTTPS -> any
TCP
WLAN net
*
*
21 (FTP)
WLAN FTP -> any
TCP
WLAN net
*
*
22 (SSH)
WLAN SSH -> any
TCP
WLAN net
*
172.32.1.254
8000
WLAN CP red -> 172.32.1.254
pass
block
reject
log
pass (disabled)
block (disabled)
reject (disabled)
log (disabled)
Hint:
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.
m0n0wall® is © 2002-2008 by Manuel Kasper. All rights reserved. [view license]

Diese Regel öffnet nun folgende Ports für das neue, integrierte WLAN: (oder auch weitere optinale OPT Ports)

- TCP/UDP 53 DNS für DNS Requests
- TCP 80 für Webtraffic HTTP
- TCP 443 für gesicherten Webtraffic HTTPS
- TCP 21 für FTP
- TCP 22 für SSH
- TCP 8000 (ACHTUNG: **TCP 8002** ab Release 2.2 !!) für das Captive Portal **(wichtig wenn Hotspot hier aktiv sein soll !!!)**

Ggf. sind für Email Verkehr noch SMTP und POP3 und IMAP und deren Secure SSL Varianten freizugeben nach demselben Schema !
Das sind dann die folgenden Ports
TCP 25 (SMTP), TCP 110 (POP3), TCP 143 (IMAP) bzw. deren Secure Varianten: Secure SMTP (SSMTP) - TCP 465 oder neuere Server benutzen auch TCP 587, Secure IMAP (IMAP4-SSL) - TCP 585, IMAP4 over SSL (IMAPS) - TCP 993, Secure POP3 (SSL-POP) - TCP 995
Wer noch andere Ports wie z.B. VPN Nutzung usw. oder auch generell alles freigeben will muss die FW Regel entsprechend anpassen !!!
(Siehe auch diesen_Thread zu dem Thema !)

Ein weiteres wichtiges Wort zu den Firewall Regeln da dies hier immer wieder Folgethreads eröffnet:
Firewall Regeln werden immer **der Reihe nach** (von oben nach unten) abgearbeitet und gelten NUR für **eingehenden** Traffic am Interface !
Das ist zwingend zu beachten und führt zu zahlreichen Fehlern wenn jemand z.B. gleich am Anfang allen TCP Traffic verbietet und nacher TCP 80 (HTTP, Web) wieder erlaubt ! Sowas funktioniert nicht, die logische Reihenfolge der Regeln ist also essentiell wichtig und sollte immer beachtet werden.

Wenns klemmt hilft in der Regel immer ein Blick ins *Firewall Log* oder Captive Portal Log. Dort wird immer angezeigt welche Ports geblockt sind und ggf. eine korrekte Funktion verhindern.
Ein Blick da rein kann also nie schaden zum Troubleshooting und schont die Nerven der Forumsuser.
Das obige Kapitel zum richtigen Setzen der FW Regeln hilft zusätzlich.
Bei Gastnetzen gilt generell besser erstmal alles verbieten und nur das öffnen was man wirklich erlauben will.

Wenn gar nichts mehr geht....(Troubleshooting)

Das ALIX Board hat einen seriellen Terminal Anschluss (9 polige DB-9 Buchse) den man mit einem seriellen Terminal Programm wie dem Windows eigenen Hyperterm oder besser TeraTerm, oder dem Klassiker PUTTY oder Linux Minicom oder Apple Mac Z-Term bedienen kann.
Seriellen COM Port am PC, Linux oder Apple Mac mit dem seriellen Port (9 pol Sub-D Buchse) mit einem seriellen **RS 232 Nullmodem Kabel** (DB-9 Weibchen an beiden Kabelenden) verbinden und im Terminal Programm die seriellen Parameter: **115.200 Baud bei pfSense**
8 Datenbits
1 Stopbit
Keine Parity
Keine Flusskontrolle
einstellen für den COM Port (serieller Port)
Wer einen Apple Mac besitzt oder an neueren PC/Laptops keinen seriellen COM Port mehr hat, benutzt einfach einen preiswerten USB_Seriell_Adapter (andere Variante) oder kabellos den jeder PC Shop um die Ecke für ein paar Euro hat.
Schaltet man dann das ALIX Board mit angeschlossenem Terminalkabel an, erhält man nun im Terminal exakt dieselben Boot Meldungen wie am PC Bildschirm und kann das Board konfigurieren und troubleshooten z.B. wenn man einmal das Zugangspasswort oder die Konfig IP Adresse vergessen hat.
Wichtig ist hier auch oft die Zuordnung der ALIX LAN Ports **vr0 = LAN, vr1 = WAN** bei der Erstinbetriebnahme.
Ebenso kann man das Board über das Terminal wieder auf seine Werkseinstellungen zurücksetzen !
Keine Angst: Das Terminal ist kein Muss !
Alles Management lässt sich auch bequem über das Webinterface einstellen und ist der Standard Konfigurations Zugang.
Die Konsole ist aber sehr hilfreich um dem ALIX Board etwas *auf die Finger zu schauen* und erleichtert die Fehlersuche, deshalb ist es generell immer empfehlenswert die paar Euro in einen USB-Seriell Adapter zu investieren.
Es gibt ebenfalls ALIX Boards inkl. VGA und Tastatur Port. Ist aber letztlich eine überflüssige Investition denn man nutzt diese nie im produktiven Dauerbetrieb.

```
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host

Enter a number: interrupt storm detected on "irq9:"; throttling interrupt source



*** This is m0n0wall, version 1.3b15
    built on Sat Oct 11 18:48:04 CEST 2008 for embedded
    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   -> vr0
    WAN   -> vr1
    OPT1  -> ath0 (OPT1)


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

Enter a number: 1

Valid interfaces are:

vr0     00:0d:b9:13:fc:3c   (up)   VIA VT6105M Rhine III 10/100BaseTX
vr1     00:0d:b9:13:fc:3d   (up)   VIA VT6105M Rhine III 10/100BaseTX
vr2     00:0d:b9:13:fc:3e          VIA VT6105M Rhine III 10/100BaseTX
ath0    00:0b:6b:2e:1c:6a          Atheros 5212

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.
```

Update zur unten folgenden Threadhistorie dieses Tutorials

Im Laufe der Zeit und bei der Fülle der Follow Up Kommentare unten zum hiesigen Tutorial sind noch einige Fragen offen geblieben oder können durch neue Features anders gelöst werden.
Es lohnt dennoch die Kommentar Threads hier zu lesen, da sie noch eine Fülle von Tips enthalten.
Für einige in den unten folgenden Threads angesprochenen Anforderungen, gibt es neue oder verbesserte Lösungsansätze:

ACHTUNG: Ab dem Release 2.2 ist der Captive Portal Port auf TCP 8002 geändert worden !
Bei allen die nach dem Update auf die 2.2 die Portalseite nicht mehr sehen unbedingt in den Firewall Regeln am Captive Portal Port die Regel von TCP 8000 auf **TCP 8002** ändern !
Wer abwärtskompatibel bleiben möchte mit dem Setup setzt eine **Range von Port TCP 8000 bis 8002** in der FW Regel !

1.) Mehrere CPs auf einer Firewall gleichzeitig aktivieren:
Ein Punkt der Folgethreads ist der Wunsch das Captive Portal auf mehrere Interfaces der Firewall zu aktivieren. Dies war bei der Erstellung des Threads in der Software nicht supported.
Diese Option ist aber seit längerem mit der Version 2.0 der pfSense gelöst. Hier hat man jetzt die Option mehrere Captive Portal Profile zu erstellen und so das Captive Portal auch für mehrere Interfaces gleichzeitig zu aktivieren um z.B. mehrere unabhängige Gastnetze auf einer Hardware zu betreiben.

2.) Isolation von Clients untereinander in Gastnetzen:
Öfter, und auch berechtigterweise, tauchte die Frage auf wie man WLAN oder auch LAN Clients untereinander in einem offenen Gast WLAN voneinander isolieren kann.
Clients bekommen ohne entsprechende Authentisierung ja erstmal keinen Zugang nach außen Richtung Internet, sind aber dennoch gemeinsam in einem IP Netz, „sehen“ sich also untereinander im Netz was "Spielkinder" reizt mal den Port Scanner anzuschmeissen und etwas zu *schnüffeln*.
Man muss vorab erst einmal generell für den Betrieb festlegen ob man sowas supporten will oder nicht in seinem Gastnetz. Bei JA ist nichts weiter zu tun. Auch in kommerziellen Hotspots in Hotels, Flughäfen ist solche Client Isolation leider nicht immer aktiv. Jeder kennt die damit verbundenen Gefahren.
Es gibt 2 Möglichkeiten einer Lösung wenn man es NICHT will das Gast Clients untereinander lokal kommunizieren können:

- 1.) Fast alle modernen Access Points (auch billige) bieten im WLAN Setup eine sog. *"Client Isolation"* Option. Diese muss man zwingend aktivieren, dann ist eine Client zu Client Kommunikation schon von vorn herein sicher ausgeschlossen.
- 2.) Sind LAN Switches beteiligt, d.h. sind die Gäste auch per Kabel angeschlossen, aktiviert man auf diesen Switches die sog. PVLAN (Private- oder Isolated VLAN) Funktion !

Das bedeutet technisch das an Client Ports in diesem betreffenden VLAN keine Broadcasts und damit auch kein ARP an Client Ports geforwardet werden sondern nur auf dem dedizierten Uplink Port. Durch das dann fehlende ARP wird eine Client zu Client Kommunikation untereinander ebenfalls sicher unterbunden !
In einem PVLAN (Isolated VLAN) wird dann ein Uplink Port definiert der auf die Firewall geht und so den Zugang nach außen realisiert.
Auf den Support dieses PVLAN Features ist bei Anschaffung solcher LAN Switches zwingend zu achten wer das benötigt !

3.) User Logging und Voucher Verwaltung:
Für kleinere und mittlere Gastnetze lässt sich ein preiswertes User Logging z.B. mit einem Raspberry Pi erledigen. Logging kann auch auf ein bestehendes NAS (QNAP, Synology) gemacht werden oder auf einem remoten Server z.B. per VPN.
Ein kleiner lokaler Server wie z.B. der RasPi kann gleichzeitig noch ein Voucher Server sein der die Gast WLAN Voucher (Einmalpasswörter) bequem über eine Weboberfläche verwaltbar macht oder das Gäste dieses selber per SMS über die Portal Webseite anfordern können.
Damit können auch nicht ITler wie z.B. Empfangs- und Tresenpersonal usw. ganz einfach diese Voucher verwalten. Anleitungen dazu findet man hier:
Voucher für pfSense online verwalten und optional Voucher per SMS verschicken
und hier
Netzwerk Management Server mit Raspberry Pi

4.) Funktions Erweiterung mit Plugins (pfSense):
Mittlerweile supportet auch die embedded Version von pfSense (nanobsd) über den Package Manager zuladbare Plugins oder Module. Hier kann man nun auch bei Bedarf Funktionen wie Proxy Server (Squid), Radius Authentisierung, dynamisches Routing (RIP, OSPF usw.) und diverse andere Zusatzoptionen zusätzlich laden.
Im Menüpunkt „Packages“ bekommt man bei der pfSense eine Übersicht.

5.) Virtualisierung:
Images für pfSense liegen nun auch als VM Image zum Download vor und können damit auch in virtuellen Umgebungen eingesetzt werden !
Ebenso ist ein schneller Test z.B. mit dem kostenlosen VmWare Player oder Virtual Box. um sich einen Überblick zu verschaffen nun keine Hürde mehr.

Ein Wort der Warnung: Generell sollte man sich den Einsatz von Firewalls in VMs sehr gründlich überlegen. Schaffen es Benutzer dort auszubrechen liegen ihnen ggf. sensible Daten wie auf dem Silbertablet vor der Nase, da dort meist auch zentrale Server laufen.
Generell gehört eine Firewall also immer auf separate HW die z.B. mit einem ALIX Board dann wirklich sicher und preiswert zu realisieren ist.

Es wird immer wieder Detailfragen zu dem Thema geben. Dafür dann einfach, wenn nicht schon geschehen, im Forum anmelden und einen neuen Thread erstellen mit Bezug auf dieses Tutorial !

Weiterhin viel Erfolg beim Betrieb dieses vielseitigen Gast Captive Portals !

Weiterführende Links

Feste Appliance Lösung (ALIX)
https://www.administrator.de/contentid/149915

Tips: Dual Radio WLAN Erweiterung mit 2,4Ghz und 5 Ghz WLAN miniPCI Karte
https://www.administrator.de/forum/wlan-karte-in-pfsense-einrichten-und- ...

Gast Passwörter (Voucher) per Webbrowser und SMS verwalten
https://www.administrator.de/contentid/193763

Gast Passwörter (Voucher) per Webbrowser und Ticket Drucker ausgeben
https://www.administrator.de/wissen/captive-portal-plus-pfsense-voucher- ...

Logging u. Voucher Server zum User Tracking
https://www.administrator.de/contentid/191718

VLAN Routing bzw. Integration in Netzwerke mit 802.1q VLANs und Multi SSID:
https://www.administrator.de/index.php?content=110259

Zentrale Benutzer Authentisierung über Radius:
https://www.administrator.de/contentid/154402