TEC WORKSHOP

Link: https://www.tecchannel.de/a/sicheren-gastzugang-fuer-lan-und-wlan-realisieren,1768961

Captive Portal mit M0n0wall
Sicheren Gastzugang für LAN und WLAN realisieren

Datum: 12.08.2008
Autor(en): Mike Hartmann

Wer einen Internetzugang für Gäste einrichten will, muss sein LAN vor unbefugten Zugriffen abschotten. Die kostenlose FreeBSD-Firewall M0n0wall bietet mit dem sogenannten Captive Portal eine komfortable und einfach einzurichtende Hotspot-Lösung.

Das Captive Portal leitet Benutzer zunächst auf eine Webseite, auf der sie Zugangsdaten eingeben müssen, bevor sie ins Internet gelangen. Damit lassen sich auch – spannend für Hotels oder Gaststätten – Lösungen realisieren, in denen ein Voucher verkauft wird, das dann einmal gültige Zugangsdaten enthält. Ähnliche Lösungen sind auch für viele WLAN-Router via Firmware verfügbar; diese kosten allerdings oft eine Menge Geld.

Als Basis für diese Konfiguration verwenden wir die kostenlose Firewall **M0n0wall**[1]. Diese mit weniger als 6 MByte extrem kleine FreeBSD-Distribution lässt sich problemlos auf älteren Systemen verwenden und von Compact Flash oder USB starten. Zudem bietet sie neben dem Captive Portal viele interessante Features wie VLAN-Support, IPsec- und PPTP-VPN, DynDNS, Traffic Shaping und Wake on LAN.

Die Mindestanforderungen an das zu verwendende System sind sehr moderat, da die M0n0wall zur Verwendung auf Embedded Systemen ausgerichtet ist. Ein Pentium III und 64 MByte RAM reichen für eine 100-MBps-Netzwerkverbindung. Soll ein Gigabit-Link bedient werden, empfiehlt der Programmierer einen P4 mit 2,4 GHz. Als Boot-Medium haben Sie die Wahl zwischen CD-ROM, USB oder Festplatte. Letztere können Sie mittels eines Adapters auch durch eine CF-Karte ersetzen. Dazu sind mindestens zwei LAN-Ports erforderlich.

1. Installation der M0n0wall

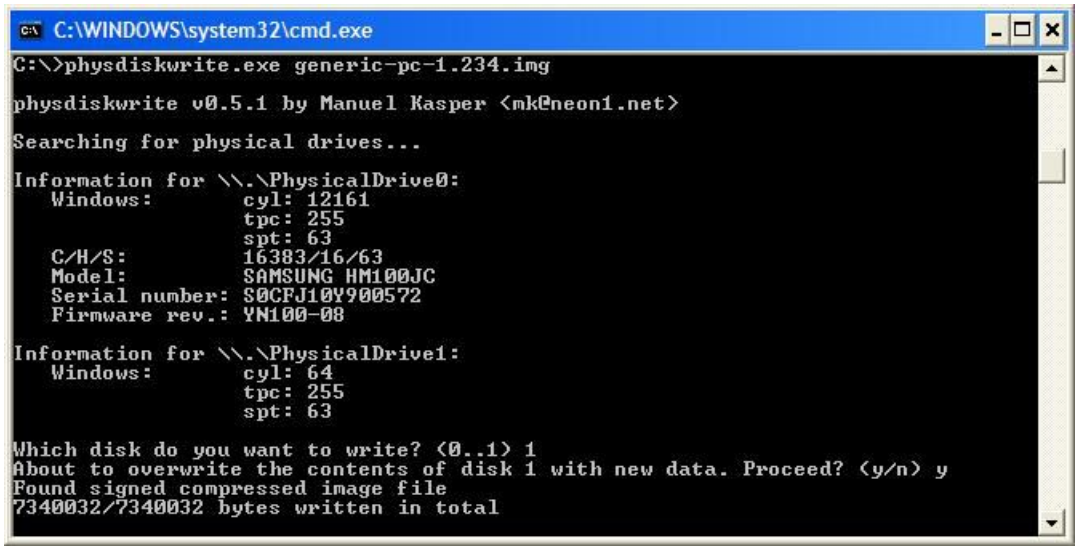
Die grundlegende Installation der M0n0wall geht recht schnell vonstatten. Nach dem Download des **Images**[2] (raw CF/HD image for generic PCs) wird dieses mit dem ebenfalls auf der Website zu findenden Tool physdiskwrite auf USB oder Harddisk geschrieben.

```
physdiskwrite <name des images>
```

Das Tool zeigt Ihnen eine Auswahl der gefundenen Datenträger. Achten Sie darauf, den richtigen auszuwählen. Unter Linux verwenden Sie statt physdiskimage einfach die Befehlszeile

```
gunzip -c <name des images> | dd of=/dev/XXX bs=16k
```

Ersetzen Sie dabei das XXX durch den Gerätenamen des Speichermediums, beispielsweise hda.



Konzentration: Bei einer Falscheingabe, ruinieren Sie die Daten auf der Festplatte.

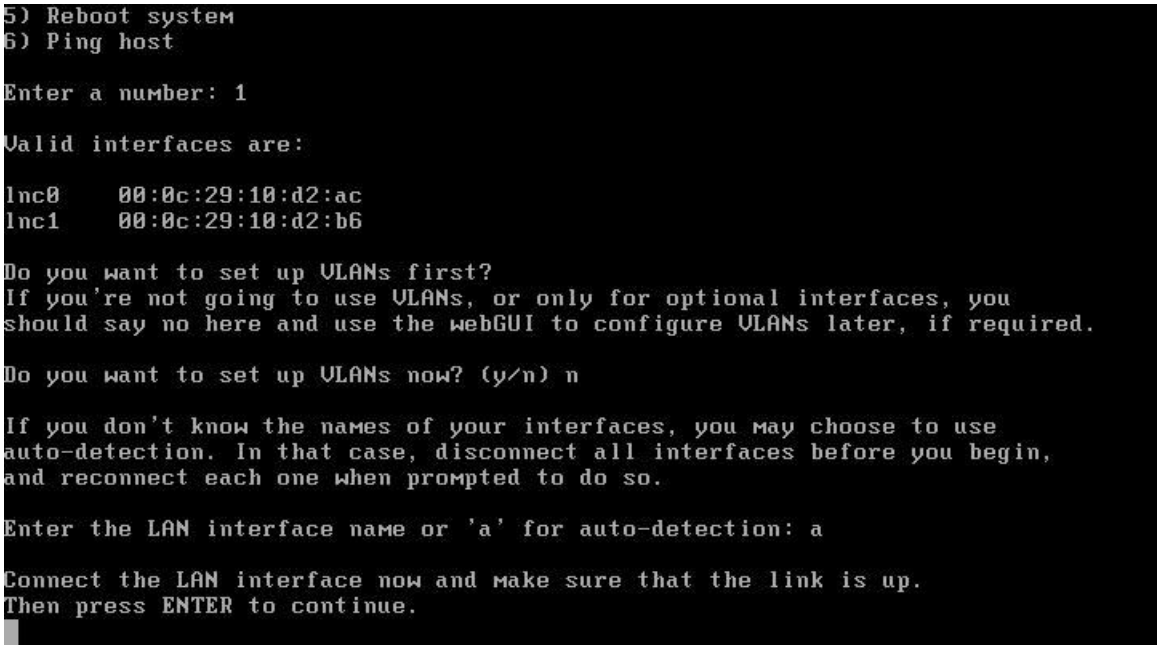
Wenn Sie ein CD-ROM im Router-System haben, können Sie auch das CD-Image der M0n0wall herunterladen und brennen.

2. Erster Start der M0n0wall

Danach sind Sie schon bereit für die Einrichtung des Systems. Im Falle eines Starts von CD-ROM benötigen Sie zusätzlich noch einen USB-Stick für die Speicherung der Konfigurationsdaten. Das Medium muss mit FAT formatiert sein. Nun können Sie die M0n0wall booten, und ein kurzer Wizard führt Sie durch die grundlegende Einrichtung. Die Schritte sind ganz einfach:

Als Erstes sind die Schnittstellen einzurichten, denen Sie auch gleich ihre Funktion zuweisen. Dabei steht LAN für das lokale Netzwerk, WAN für den Weitverkehrszugang und OPT für sonstige Netzwerke. In diesem Fall wird das Gastnetz als LAN konfiguriert und die Verbindung ins Internet als WAN.

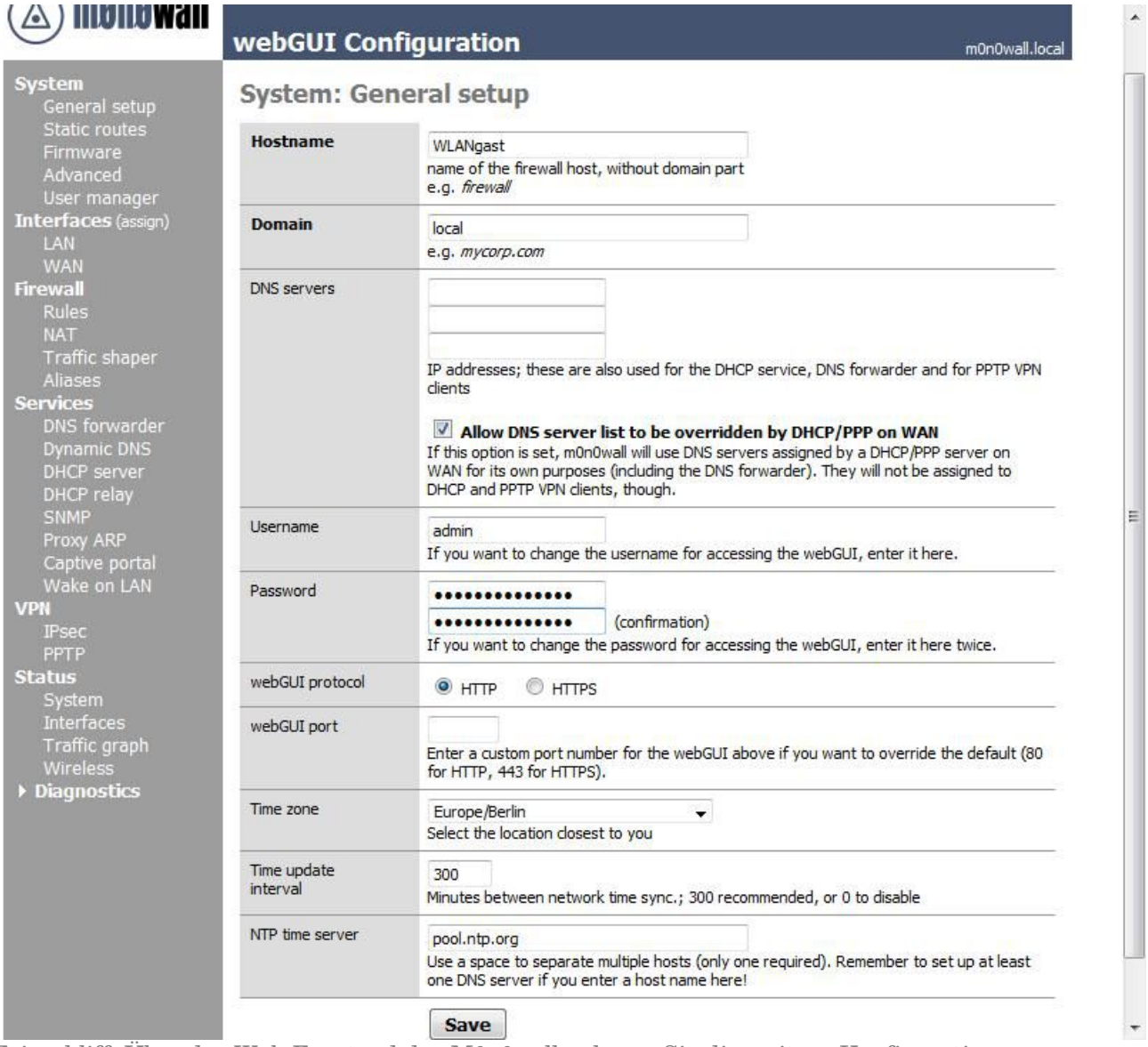
Mittels der Funktion „autodetect“ erleichtert M0n0wall das Identifizieren der Schnittstellen. Dazu sollte zunächst kein Kabel angeschlossen sein. Erst wenn das System Sie dazu auffordert, schließen Sie das jeweilige Netzwerkkabel an. M0n0wall entdeckt den Statuswechsel (link-up) an der Netzwerkkarte und identifiziert diese richtig. Klappt das nicht, müssen Sie über den Namen der Karte gehen. Hinweise zur Benennung der Karten gibt das **M0n0wall-Handbuch**[3].



Suche: Die Zuordnung der Netzwerkschnittstellen gestaltet sich nicht ganz einfach, ist aber auch kein Hexenwerk.

Danach ist ein Reboot fällig. Im Anschluss können Sie im **zweiten Schritt** die LAN-Adresse ändern und den DHCP für die LAN-Clients konfigurieren.

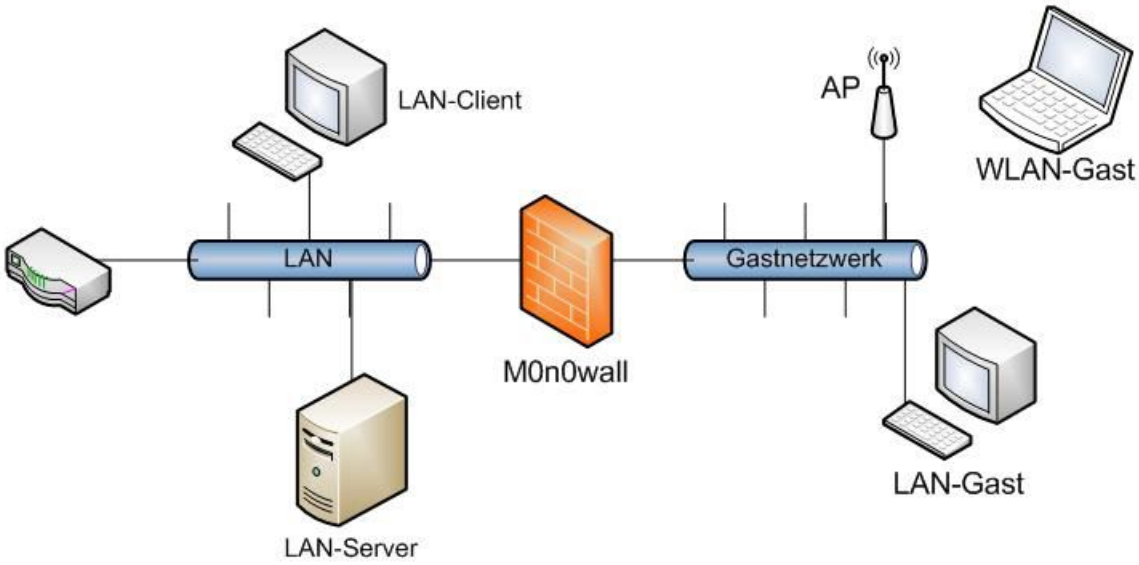
Die **weitere Konfiguration** erfolgt über die Web-Schnittstelle der M0n0wall. Dazu rufen Sie einfach von einem Rechner im Gastnetz die URL http://192.168.1.1 auf, sofern Sie die IP-Konfiguration des LAN-Adapters nicht geändert haben. Der Benutzername ist admin und das dazu passende Kennwort mono. Letzteres sollten Sie umgehend unter „General Setup“ ändern.



Feinschliff: Über das Web-Frontend der M0n0wall nehmen Sie die weitere Konfiguration vor.

3. Konfiguration

Ziel unserer Lösung ist es, ein separates Netzwerksegment zu erzeugen, in dem die für Gäste zugänglichen Access Points durch die M0n0wall vom Firmen-LAN abgeschottet sind. Daher gestaltet sich die Einrichtung des WAN-Interfaces wie folgt: Die M0n0wall soll von einem DHCP-Server im Firmennetz eine IP-Adresse sowie die sonstigen Parameter wie Default Gateway und DNS-Server beziehen. Dazu stellen Sie unter „Interfaces / WAN“ den Eintrag „Type“ auf DHCP.



Abgeschottet: Die Gäste sollen sich in einem eigenen Segment tummeln.

Im nächsten Schritt wird die Hotspot-Funktion scharf geschaltet. Dazu rufen Sie das Menü „Services / Captive portal“ auf und schalten das „Captive portal“ ein. Die Schnittstelle sollte LAN sein, denn an diesem Segment hängen die Gäste.

Unter „Authentication“ stellen Sie „Local user manager“ ein. Damit überlassen Sie die Benutzerverwaltung der M0n0wall. Wichtig ist, dass Sie bei „Portal page contents“ eine HTML-Seite hochladen, damit das Login funktioniert. Eine solche Seite könnte beispielsweise so aussehen:

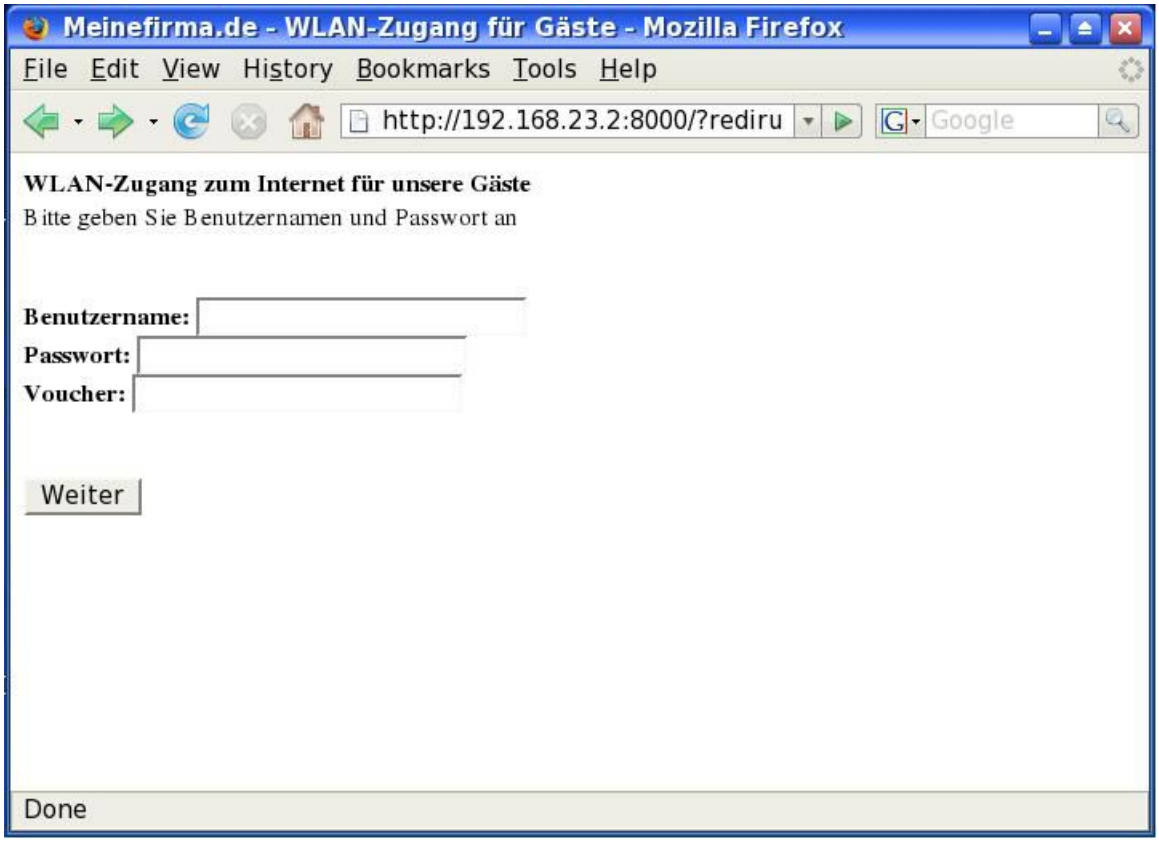
```
<html>
<head><title>Meinefirma.de - WLAN-Zugang für Gäste</title></head>
<body>
<b>WLAN-Zugang zum Internet für unsere Gäste</b><br/>
Bitte geben Sie Benutzernamen und Passwort an oder Ihren Voucher-Code<br/><br/>
<form method="post" action="$PORTAL_ACTION$"><br/>
<b>Benutzername:</b><input name="auth_user" type="text"https://www.computerwoche.de/><br/>
<b>Passwort:</b><input name="auth_pass" type="password"https://www.computerwoche.de/><br/>
<!-- nur in der aktuellen Beta von M0n0wall -->
<b>Voucher:</b><input name="auth_voucher" type="text"https://www.computerwoche.de/><br/><br/><br/>
<input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$"https://www.computerwoche.de/>
<input name="accept" type="submit" value="Weiter"https://www.computerwoche.de/>
</form></body></html>
```

4. Aktivieren des Hotspots

Nach dem Speichern der Änderungen können Sie über den integrierten Benutzermanager verschiedene User anlegen – achten Sie aber darauf, dass Sie den Tab „Users“ bei „Services / Captive portal“ verwenden und nicht den generellen Benutzer-Manager der M0n0wall („System / User manager“). Wenn Sie die aktuelle Beta-Version installiert haben, können Sie auch das Voucher-System nutzen – etwa für eine Gaststätte. Die Einrichtung und Nutzung des Voucher-Systems ist im M0n0wall-Handbuch **detailliert beschrieben**[4].

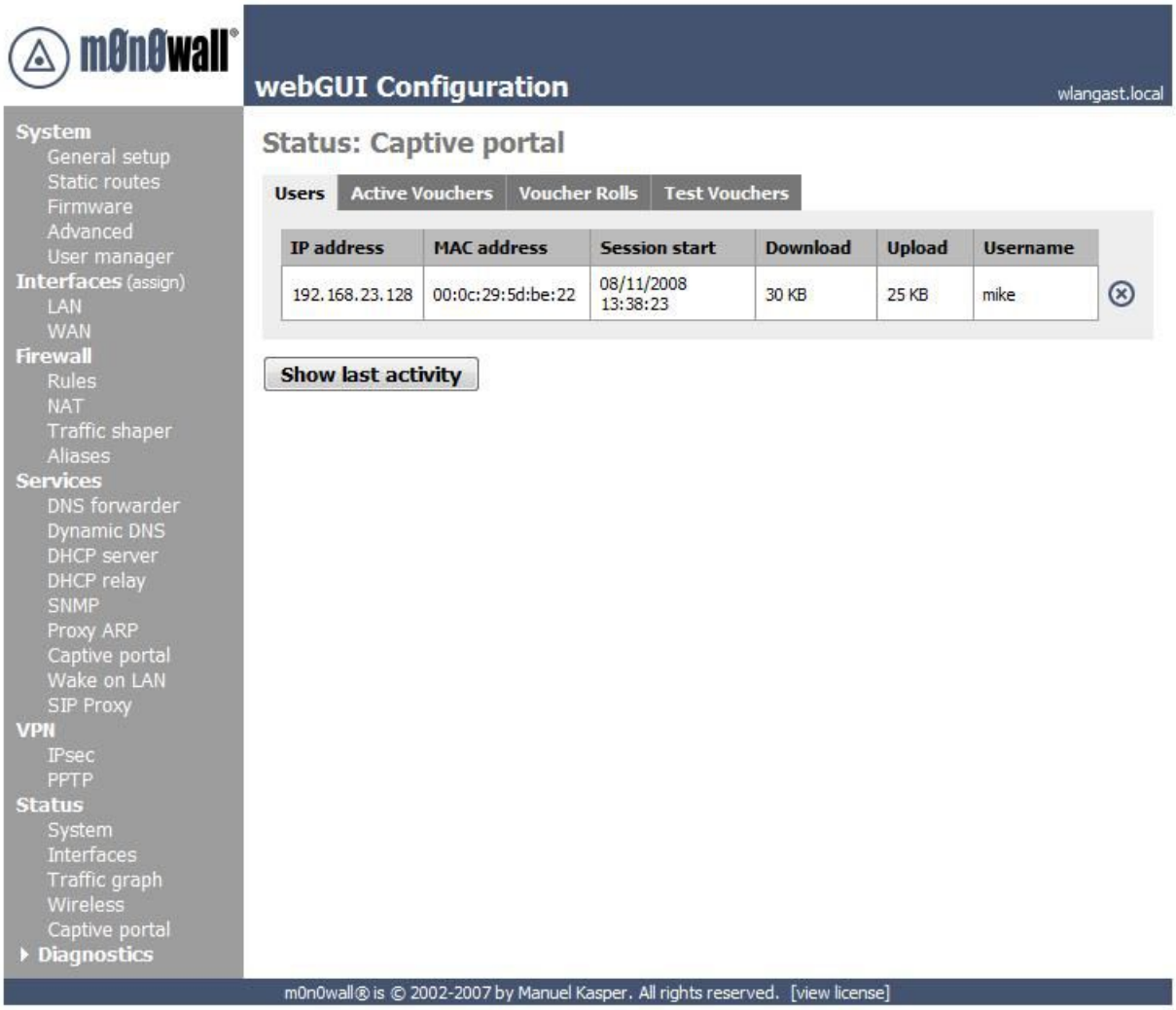
Wer darf: Im integrierten Benutzer-Manager legen Sie die User-Kennungen an, die über den Hotspot das Internet nutzen dürfen.

Damit sind die grundlegenden Arbeiten erledigt. Wenn Sie jetzt von einem Rechner im Gastnetz aus das Internet nutzen wollen, gelangen Sie zunächst zur Anmeldemaske. Erst nach Eingabe der richtigen Daten können Sie weitersurfen.



Nicht schön, aber funktional: Das Login für den Hotspot. Sie sollten etwas mehr Mühe in das Design investieren als wir.

Über das Menü „Status / Captive portal“ können Sie nun jederzeit einsehen, was gerade in Ihrem Gastnetz passiert. Über „Status / Traffic“ erhalten Sie ständig aktuelle Informationen über den Datenverkehr. Wenn Sie verhindern wollen, dass Ihre Gäste zu viel Bandbreite verbrauchen, können Sie später noch das Traffic Shaping aktivieren („Firewall / Traffic shaper“).



Status: M0n0wall gibt einen aktuellen Überblick über die Hotspot-Funktionen.

5. Sicherheitsregeln und Add-ons

Zu guter Letzt sollten Sie noch ein paar Firewall-Regeln erstellen, die die Möglichkeiten der Gäste einschränken. Zunächst sollten Sie den Zugriff auf Ihr LAN ausschließen – die Gäste dürfen lediglich mit dem Internet kommunizieren. Welche Protokolle Sie zulassen wollen, bleibt Ihnen überlassen. Machen Sie sich aber die jeweils möglichen Konsequenzen klar. Wenn Sie außer HTTP, HTTPS und POP3 beispielsweise noch SMTP freigeben, besteht die Gefahr, dass über Ihr Netzwerk massenhaft Spam versendet wird.

Da die Web-GUI der M0n0wall über das LAN erreichbar ist, sollten Sie abgesehen vom geänderten Passwort auch den Port verändern, auf dem der Web-Server lauscht. Oder Sie richten über „Firewall / NAT“ eine Regel ein, die WAN-Traffic (also aus dem Firmennetz) auf die LAN-IP der M0n0wall (also das Gastnetz) weiterleitet. Dann können Sie aus Ihrem Firmennetz heraus die M0n0wall verwalten.

Der Speicherplatz ist bei einer M0n0wall-Installation auf Compact Flash stark beschränkt. M0n0wall bietet jedoch zum Glück die Möglichkeit, Log-Einträge an einen externen Syslog-Server zu schicken. Ein solcher ist bei Linux schon integriert, für Windows gibt es mit dem **Kiwi-Syslog-Daemon**[5] einen kostenlosen Syslog-Server für Windows. (mha)

Links im Artikel:

[1] **http://m0n0.ch/wall/**

[2] **http://m0n0.ch/wall/downloads.php**

[3] **http://doc.m0n0.ch/handbook/hardware-sizing.html%202.5.2**

[4] **http://doc.m0n0.ch/handbook/ch12s04.html**

[5] **http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/**
